Elementary Divisors Over Rings

by

Ahmad Abdulaziz Al-Dharrab

A Thesis Presented to the

FACULTY OF THE COLLEGE OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

MATHEMATICS

January, 1979

Order Number 1355712

Elementary divisors over rings

Al-Dharrab, Ahmad Abdulaziz, M.S.

King Fahd University of Petroleum and Minerals (Saudi Arabia), 1979

U·M·I

300 N. Zeeb Rd.
Ann Arbor, MI 48106

ELEMENTARY DIVISORS OVER RINGS

by

Ahmad Abdulaziz Al-Dharrab

A Thesis Presented to the

FACULTY OF THE GRADUATE SCHOOL

UNIVERSITY OF PETROLEUM AND MINERALS
DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the

Requirements for the Degree

MASTER OF SCIENCE IN MATHEMATICS

January 2, 1979

UNIVERSITY OF PETROLEUM AND MINERALS

DHAHRAN : SAUDI ARABIA

This thesis, written by

Mr. Ahmad Abdulaziz Al-Dharrab

under the direction of his Thesis Committtee, and approved by all its members, has been presented to and accepted by the Dean of the Graduate School, in partial fulfilment of the requirements for the degree of

Master of Science in Mathematics

Dean of the Graduate School

Date 29/1/79

M. Sunkar

Department Chairman

Thesis Committee

4/2/1399 H

Jan. 2nd '79

Chairman

Jan 2, 1979

Member

2/1/1979

Member

4/2/1399 H

بسم الله الرحمن الرحيم

ACKNOWLEDGEMENTS

This research could not have been accomplished without the help and consistent encouragement of all those who contributed to my learning process during my stay in the University of Petroleum and Minerals. I wish to express my sincere thanks to Dr. S.M. Fakhruddin who supervised this work and helped me a great deal in improving the quality of this thesis. I am particularly indebted to Professor S.M. Yahya for his guidance and helpful directions. I would also like to thank Dr. Ali Al-Daffa' for his consistent encouragement and interest in this work.

Finally, I would like to thank Mr. Mohammad Ayub Khan for the patience he showed in typing the thesis.

TABLE OF CONTENTS

ABSTRACT

In our thesis we plan to systematically present the theory of reduction to a diagonal form of a matrix over an arbitrary ring. This work is based mainly on Kaplansky's paper "Elementary Divisors and Modules".

CHAPTER 0

INTRODUCTION

This thesis gives a systematic account of generalization in the setting of rings of some reduction processes of matrices over a field: namely, we study the conditions over a ring under which a given rectangular matrix over that ring is triangulizable or diagonalizable.

We give below a summary of the thesis.

In chapter I we present the basic generalities in rings, ideals and modules. We also present a brief account of divisibility in integral domains. In the last section of this chapter we also introduce the notion of a Bezout domain, and conclude this section by giving an example, due to Cohn, of a Bezout domain which is not a principal ideal domain.

In chapter II we present the basic notions of matrices, determinants, ... etc., over a commutative ring with identity. In particular, we define the determinant function on $Mat_n R$ to be the unique alternating R-multilinear form $d: Mat_n R \to R$ such that $d(I_n) = 1_R$.

Chapter III contains the main body of the thesis. In the first section we define the notions of triangular and diagonal reductions of a matrix over a commutative ring. A Hermite ring is a ring over which every 1×2 matrix admits a diagonal reduction. In section 2 we study Hermite rings and we present some of their basic properties. This section concludes with a theorem characterizing a Hermite ring. This theorem is due to Gillman and Henriksen. In section 3 we study triangular reduction. The main result of

this section is that triangular reduction is possible over a Hermite ring. Interalia we also prove that if R is a Hermite ring so is R_n - the ring of $n \times n$ matrices over R. In section 4 we study matrices over F-rings. In the fifth section we show that the classical theory of reduction of skew symmetric matrices is valid over commutative Hermite rings. In section 6 we introduce and study elementary divisor rings, and prove a theorem giving a necessary and sufficient condition for a ring to be an elementary divisor ring. This result is due to Gillman and Henriksen. We also give an example of a Hermite ring which is not an elementary divisor ring and another example of an F-ring which is not a Hermite ring. In the concluding section we show that the class of elementary divisor rings is fairly large by showing that a von Neumann regular ring is an elementary divisor ring.

CHAPTER I

GENERALITIES ON RINGS

Notions of Zero Divisors

1.1.1 Definition: A ring R is an ordered triple $(R, +, .)$ consisting of a non-empty set R with two binary operations, addition '+' and multiplication '.' such that:

R1. $(R, +)$ is an abelian group.

R2. $(ab)c = a(bc)$ for all $a, b, c \in R$ (multiplication is associative).

R3. multiplication is distributive over addition on both sides,

$$\left.\begin{aligned} \text{i.e.,}\quad a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned}\right\} \text{ for all } a, b, c \in R.$$

Remark: (i) A commutative ring is a ring $(R, +, .)$ in which multiplication is commutative, i.e., $a \cdot b = b \cdot a$ for all $a, b \in R$.

(ii) A ring with identity is a ring $(R, +, .)$ in which there exists an identity element for the operation of multiplication, represented by the symbol 1, so that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Convention: Hereafter the word ring shall mean a commutative ring with identity unless otherwise specified. Also ab will stand for $a \cdot b$.

1.1.2 Definition: An element a in a ring R is called a zero divisor if it divides zero in the sense that there exist $b(\neq 0) \in R$ such that $ab = 0$.

1.1.3 Definition: Given a ring R, an element $a \in R$ is said to be invertible, or a unit if there exists an element $b \in R$ such that $ab = 1$. In this case, we say a and b are inverses of each other.

1.1.4 Definition: A commutative ring R with identity $1 \neq 0$ having no non-zero zero divisors is called an integral domain.

Remarks: (i) An integral domain has at least two elements (namely 0 and 1).

(ii) A ring R is an integral domain if the set of its non-zero elements R^* is closed under multiplication.

1.1.5 Examples: (i) If Z, Q, R and C denote the sets of integers, rationals, real numbers, and complex numbers respectively, then the systems

$$(Z, +, .), \ (Q, +, .), \ (R, +, .), \ (C, +, .)$$

are all examples of rings (where `+' and `.' are taken to be ordinary addition and multiplication).

(ii) The ring Z of integers is an integral domain.

(iii) Given any ring R, we consider the set $M_n(R)$ of $n \times n$ matrices over R. If $I_n = \{1, 2, \ldots, n\}$, a typical element

of $M_n(R)$ is a function $f: I_n \times I_n \to R$, which is denoted by $f(i, j) = a_{ij}$ and which can be arranged as an $n \times n$ square array

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \quad (a_{ij} \in R).$$

For the sake of simplicity, let us abbreviate the $n \times n$ matrix whose (i, j)th entry is a_{ij} by (a_{ij}). The set $M_n(R)$ is a ring, under the following operations of addition and multiplication:

$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ and $(a_{ij})\,(b_{ij}) = (c_{ij})$ where

$$c_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj}.$$

The zero element of $M_n(R)$ is the $n \times n$ matrix, all of whose entries are 0, and $-(a_{ij}) = (-a_{ij})$.

(iv) The $n \times n$ matrices over Q (or R or C) form a non-commutative ring with identity.

(v) An example of a ring with zero divisors is Z_n, where the integer $n > 1$ is composite; if $n = n_1 n_2$ in Z $(1 < n_1, n_2 < n)$, then the product $n_1 \cdot n_2 = 0$ in Z_n but $n_1 \neq 0$, $n_2 \neq 0$.

1.2 Quotient Rings and Ideals

1.2.1 **Definition:** A subset S of a ring R is a subring if it is itself a ring under the induced operations of R.

1.2.2 **Definition:** An ideal $\mathfrak{a}$ of R is a subset of R which is a subgroup of the additive group of R and $R\mathfrak{a} \subseteq \mathfrak{a}$, i.e., for all $x \in R$ and all $a \in \mathfrak{a}$, we have $xa \in \mathfrak{a}$. Note that $\mathfrak{a}$ is a subring of R.

1.2.3 **Definition:** Let $\mathfrak{a}$ be an ideal of a ring R. Then the set $R/\mathfrak{a} = \{x + \mathfrak{a} \mid x \in R\}$ forms a ring under the following well defined operations:

$$\left.\begin{aligned} (x + \mathfrak{a}) + (y + \mathfrak{a}) &= (x + y) + \mathfrak{a} \\ (x + \mathfrak{a})\,(y + \mathfrak{a}) &= xy + \mathfrak{a} \end{aligned}\right\} \text{ for every } x, y \in R.$$

This ring is called the quotient ring of R by the ideal $\mathfrak{a}$.

1.2.4 **Example:** Let R be a ring. For each $x \in R$, let xR (or Rx) denote the set of multiples of x in R, i.e., the set of elements of the form ux, $u \in R$. This set xR (or Rx) is an ideal.

1.3 Principal and Prime Ideals

1.3.1 Definition: A principal ideal (x) (or Rx) is the ideal generated by x, i.e., it consists of all elements of the form ax, $a \in R$.

1.3.2 Definition: An ideal $\mathfrak{P}$ in R is prime if $\mathfrak{P} \neq (1)$ and if $xy \in \mathfrak{P}$, then either $x \in \mathfrak{P}$ or $y \in \mathfrak{P}$.

1.3.3 Examples: (i) The zero ideal in an integral domain is prime since $ab = 0$ if and only if $a = 0$ or $b = 0$.

(ii) If p is a prime integer, then the principal ideal (p) in z is prime since $ab \in (p)$ iff $p|ab$ implies $p|a$ or $p|b$, whence $a \in (p)$ or $b \in (p)$.

Remark: A domain (integral domain) is called a principal ideal domain if all its ideals are principal. For example, Z is a principal ideal domain.

1.4 Maximal Ideals and Jacobson Radical

1.4.1 Definition: An ideal $\mathfrak{M}$ in a ring R is maximal if $\mathfrak{M} \neq (1)$ and if there is no ideal $\mathfrak{a}$ such that $\mathfrak{M} \subset \mathfrak{a} \subset (1)$. (strict inclusions).

1.4.2 Definition: A partially ordered set X is a set with a binary relation '$\leqslant$' which is reflexive ($x \leqslant x$), transitive

$(x \leq y,\ y \leq z \Rightarrow x \leq z)$ and antisymmetric $(x \leq y,\ y \leq x \Rightarrow x = y)$.

A subset C of X is a chain if $x, y \in C$ implies either $x \leq y$ or $y \leq x$, i.e., C is linearly (or totally) ordered. $m \in X$ is <u>maximal</u> if $m \leq x$ implies $m = x$. If $Y \subseteq X$, then $b \in X$ is an <u>upper bound</u> of Y in X if $y \leq b$ for all $y \in Y$.

1.4.3 <u>Zorn's Lemma</u>: If X is a partially ordered set, and if every chain in X has an upper bound in X, then X has at least one maximal element.

1.4.4 <u>Theorem (Krull's theorem)</u>: Let $\mathfrak{a}$ be a proper ideal of a ring $R \neq 0$, then there exists a maximal ideal $\mathfrak{m}$ of R containing $\mathfrak{a}$.

<u>Proof</u>: Let X be the set of all proper ideals of R containing $\mathfrak{a}$, and take '$\leq$' to be the inclusion, then X is a partially ordered set. ($X \neq \phi$ for $\mathfrak{a} \in X$). Consider a chain C in X. Form $\mathfrak{a}_1 = \bigcup_{b \in C} b$, $\mathfrak{a}_1$ is an ideal, for if $x, y \in \mathfrak{a}_1$, then there exist b_1 and $b_2 \in C$ such that $x \in b_1$ and $y \in b_2$ and since C is a chain one is contained in the other, say $b_1 \subseteq b_2$. Hence $x, y \in b_2$, so $x - y \in b_2 \subseteq Q_1$. Similarly, we can show that $\mathfrak{a}_1$ is closed under multiplication. Since $1 \notin$ any $b \in C$, so $1 \notin \mathfrak{a}_1$, i.e., $\mathfrak{a}_1$ is a proper ideal. Clearly $\mathfrak{a}_1$ is an upper bound of C in X. Hence, by Zorn's Lemma, there exists a maximal element in X, which by definition is a maximal ideal of R containing $\mathfrak{a}$.

1.4.5 Remark: $x \in R$ is a non-unit if and only if $(x) \subset R$, i.e., if and only if $(x) \subset$ some maximal ideal of R. Thus the set of all non-units of R is the union of all maximal ideals of R. Suppose that the non-units form an ideal $\mathfrak{M}$ of R, then $\mathfrak{M}$ contains every maximal ideal of R, and so $\mathfrak{M}$ is the unique maximal ideal of R, and conversely if $\mathfrak{M}$ is the only maximal ideal, then $\mathfrak{M}$ is the set of all non-units of R.

1.4.6 Definition: A ring R with exactly one maximal ideal $\mathfrak{M}$ is called a local ring.

1.4.7 Proposition: Let R be a ring and $\mathfrak{M}$ a maximal ideal of R such that every element of $1 + \mathfrak{M}$ is invertible in R. Then R is a local ring.

Proof: Let $x \notin \mathfrak{M}$. Since $\mathfrak{M}$ is maximal, then the ideal generated by x and $\mathfrak{M}$ is R = (1). Hence there exist $y \in R$ and $t \in \mathfrak{M}$ such that $xy + t = 1$, so $xy = 1 - t \in 1 + \mathfrak{M} >$ xy is an invertible $\Rightarrow$ x is invertible. Hence every element not in $\mathfrak{M}$ is invertible, so $\mathfrak{M}$ is the unique maximal ideal.

1.4.8 Definition: The Jacobson radical rad R of R is defined to be the intersection of all the maximal ideals of R, i.e.,

$$\text{rad } R = \bigcap \{\mathfrak{M} \mid \mathfrak{M} \text{ is a maximal ideal of } R\}$$

For example:

rad R in Z is 0.

1.4.9 Proposition: $x \in \text{rad } R$ if and only if $1 - xy$ is a unit in R, for all $y \in R$.

Proof: $\Rightarrow$ Suppose $1 - xy$ is not a unit for some y, then by 1.4.5, it belongs to some maximal ideal, say $\mathfrak{M}$. Now if $x \in \text{rad } R \subseteq \mathfrak{M}$, so $xy \in \mathfrak{M}$. Hence $1 - xy + xy = 1 \in \mathfrak{M} \Rightarrow \mathfrak{M} = R$ (since $1 \notin \mathfrak{M}$), this leads to a contradiction.

$\Leftarrow$ Suppose $x \notin \text{rad } R$, i.e., $x \notin$ some maximal ideal $\mathfrak{M}$ of R, then $\mathfrak{M}$ and x generate R. Thus $R = \mathfrak{M} + (x)$, and so $1 = a + xy$, $a \in \mathfrak{M}$ and some $y \in R$. Therefore $1 - xy = a \in \mathfrak{M}$ is not invertible, which is a contradiction.

1.5 Noetherian Rings.

We recall that an ideal $\mathfrak{A}$ is finitely generated if we can find a finite set $\{a_1, a_2, \ldots, a_n\}$ of elements such that

$$\mathfrak{A} = Ra_1 + Ra_2 + \ldots + Ra_n .$$

Ra_i is just another way of writing the principal ideal (a_i), which is used when we wish to emphasize that (a_1) consists of all elements of the form ra_1, where r is an arbitrary element of R.

1.5.1 Definition: A ring R is called noetherian if every ideal of R is finitely generated (after Emmy Noether).

1.5.2 Definition: The ascending chain condition is said to hold in R, if whenever we have an infinite increasing sequence

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

of ideals; there exists an integer m such that $\mathfrak{a}_n = \mathfrak{a}_m$ for all $n \geq m$.

1.5.3 Definition: The maximal condition is said to hold in R, if given any non-empty set W of ideals of R there is always an ideal $\mathfrak{a}$ in the set W such that if $\mathfrak{a}'$ belongs to W and $\mathfrak{a}' = \mathfrak{a}$, then $\mathfrak{a}' = \mathfrak{a}$.

1.5.4 Examples: (i) Every commutative principal ideal ring is noetherian.

(ii) Rings of polynomials in n variables with coefficients in a field are noetherian.

1.5.5 Theorem [N]: The following three statements are equivalent:

(1) The ascending chain condition holds in R;

(2) The maximal condition for ideals holds in R;

(3) R is noetherian.

Proof: Suppose first that the chain condition holds, and let G be a non-empty set of ideals. We shall suppose that no member of G is maximal, and hence derive a contradiction. This will prove that (1) $\Rightarrow$ (2). Since G is not empty, it contains at least one ideal; let $\mathfrak{a}_1 \in G$. By hypothesis, $\mathfrak{a}_1$ cannot be maximal; we

can therefore find $\mathfrak{a}_2 \in G$ such that $\mathfrak{a}_2 \supseteq \mathfrak{a}_1$, where the inclusion is strict. Again, since $\mathfrak{a}_2$ is not maximal, there exists $\mathfrak{a}_3 \in G$ such that $\mathfrak{a}_3 \supseteq \mathfrak{a}_2$ - and so on. this gives the required contradiction, because the sequence $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ will violate the chain condition.

Now assume that the maximal condition holds, and let $\mathfrak{a}$ be a given ideal. Denote by G the set of all finitely generated ideals contained in $\mathfrak{a}$, then G is not empty because it contains (0). If $\mathfrak{a}' = Ra_1 + Ra_2 + \ldots + Ra_n$ is an ideal of the set G which is maximal, then $\mathfrak{a}' \subseteq \mathfrak{a}$. We shall prove that $\mathfrak{a}' = \mathfrak{a}$, from which it will follow that $\mathfrak{a}$ is finitely generated, and, hence, that (2) $\Rightarrow$ (3). Now if $\mathfrak{a}' \neq \mathfrak{a}$, we can find $b \in \mathfrak{a}$ such that $b \notin \mathfrak{a}'$, and then the ideal

$$Ra_1 + Ra_2 + \ldots + Ra_n + Rb$$

will belong to G, and it will strictly contain $\mathfrak{a}'$. This, however, is impossible by the choice of $\mathfrak{a}'$.

Finally (3) $\longrightarrow$ (1). For this, suppose that every ideal is finitely generated, and let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ be an increasing sequence of ideals. If we denote by $\mathfrak{a} = \bigcup \mathfrak{a}_i$, then $\mathfrak{a}$ is an ideal; for if $x_1, x_2 \in \mathfrak{a}$ and $r \in R$, then we can find an integer ℓ such that x_1 and x_2 are both in $\mathfrak{a}_\ell$, hence $x_1 + x_2$, $x_1 - x_2$, and rx_1 are all in $\mathfrak{a}_\ell$, so that they are all in $\mathfrak{a}$. Since $\mathfrak{a}$ is an ideal, it has, by hypothesis, a finite base. Let $\mathfrak{a} = (a_1, a_2, \ldots, a_n)$ and for each i choose m_i so that

$a_i \in \mathfrak{a}_{mi}$, then all the a_i are in $\mathfrak{a}_m$, where

$$m = \max (m_1, m_2, \ldots, m_n) .$$

If now $n > m$ we have

$$\mathfrak{a} = (a_1, a_2, \ldots, a_n) \subseteq \mathfrak{a}_m \subseteq \mathfrak{a}_n \subseteq \mathfrak{a} ;$$

thus $\mathfrak{a}_n = \mathfrak{a}_m$ provided only that $n > m$.

1.5.6 Corollary: Every principal ideal domain is a noetherian ring.

1.6 Divisibility in Integral Domains

In this section we present the classical theory of divisibility and factorization of elements in an integral domain. Note that R will always denote an integral domain in this section.

1.6.1 Definition: Let a, b be two elements of R where R is an integral domain, we say a is a divisor of b (b is a multiple of a or a divides b), if there is an element $c \in R$ such that $b = ac$.

Remark: If a is a divisor of b we denote this by $a \mid b$, otherwise $a \nmid b$.

1.6.2 Theorem (Divisibility rules): Let R be an integral domain, then

(i) $1 \mid a$, $a \mid 0$, $a \mid a$ for all $a \in R$.

(ii) $a \mid 1$ iff a is a unit.

(iii) $a \mid b \Rightarrow ar \mid br$ for any $r \in R$.

(iv) $a \mid b_i$ for $i = 1, \ldots, m \Rightarrow a \mid r_1 b_1 + \ldots + r_n b_n$ for all $r_i \in R$.

(v) $a \mid b$, $b \mid c \Rightarrow a \mid c$.

(vi) $a \mid b \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$

(vii) $a \mid b$ and $b \mid a \Leftrightarrow (a) = (b) \Leftrightarrow a = bu$, where u is a unit.

Proof: (i) Since $a = a \cdot 1 \Rightarrow 1 \mid a$ for all $a \in R$.

Since $a \cdot 0 = 0 \Rightarrow a \mid 0$ for all $a \in R$.

Since $a = a \cdot 1 \Rightarrow a \mid a$ for all $a \in R$.

(ii) $\Rightarrow$ Suppose $a \mid 1$, then $1 = a \cdot c$ for some $c \in R$. By definition 1.1.3 a is a unit.

$\Leftarrow$ Suppose a is a unit, then there exist $c \in R$ such that $ac = 1$. By definition 1.6.1, $a \mid 1$.

(iii) Suppose $a \mid b$, then there is $c \in R$ such that $b = ac$.

Multiply both sides by $r \in R$. Then $br = acr = arc$.

By definition 1.6.1 $\Rightarrow ar \mid br$.

(iv) Suppose $a \mid b_1$, $a \mid b_2$, $\ldots$, $a \mid b_n$. Then by (iii) above $ar_1 \mid b_1 r_1$, $ar_2 \mid b_2 r_2$, $\ldots$, $ar_n \mid b_n r_n$. By definition 1.6.1 $b_1 r_1 = ar_1 c_1$, $b_2 r_2 = ar_2 c_2$, $\ldots$, $b_n r_n = ar_n c_n$.

Therefore

$$b_1 r_1 + b_2 r_2 + \ldots + b_n r_n = ar_1 c_1 + ar_2 c_2 + \ldots + ar_n c_n$$
$$= a[r_1 c_1 + r_2 c_2 + \ldots + r_n c_n]$$

Since $r_1c_1 + \ldots + r_nc_n \in R$,

$$a \mid r_1b_1 + r_2b_2 + \ldots + r_nb_n .$$

(v) Suppose $a \mid b$ and $b \mid c$, then by definition 1.6.1 $b = an$ and $c = bm$ for some $n, m \in R$. Therefore $c = anm$. Hence $a \mid c$, since $nm \in R$.

(vi) $a \mid b$ means $b = ac$ for some $c \in R$, thus $b \in (a)$, so that $(b) \subseteq (a)$.

Conversely, if $(b) \subseteq (a)$, then there exists an element $c \in R$ for which $b = ac$, implying that $a \mid b$.

(vii) Apply (vi) twice.

Also $a = bc$, $b = ad$, so $a = acd$.

Hence $1 = cd$, so c is a unit.

Remark: 1. By (vii) $(a) = R \iff a$ is a unit

2. Consider the relation $b = ar$ in R, then we can write this relation by introducing $1 = uu'$ where u is a unit at any place in the representation. For example;

$b = auu'r$, therefore if a is a divisor of b, then au is a divisor of b for any unit $u \in R$.

1.6.3 Definition: Let $a, b \in R$. Then a and b are associates if there exists a unit element u such that $a = bu$.

Remark: 1. If a and b are associates then we write $a \sim b$.

2. From 1.6.2 (vii) it follows that $a \sim b$ iff $a \mid b$ and $b \mid a \iff (a) = (b)$.

3. $\sim$ is an equivalence relation.

1.6.4 Definition: Let p and q be non-zero non-units of R.

(i) p is called a prime, if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

(ii) q is called irreducible, if $q = ab$ then a or b is a unit.

Remark: An element is irreducible iff every one of its divisors is an associate.

1.6.5 Theorem: Let p be a non-zero non-unit in R, then

(i) p is a prime element iff (p) is prime ideal.

(ii) p is irreducible iff (p) is maximal in the set of all proper principal ideals.

(iii) Every prime element is irreducible.

Proof: (i) $\Longrightarrow$ Let p be a prime element, let $a, b \in R$ and let $ab \in (p) \Rightarrow$ there exist $r \in R$ such that $ab = rp$, hence $p \mid ab$. By hypothesis P is a prime element, so $p \mid a$ or $p \mid b$. Therefore either $a \in (p)$ or $b \in (p)$. Thus (p) is a prime ideal.

$\Leftarrow$ Let (p) be a prime ideal, and $p \mid ab$. Then $ab \in (p)$ $\Rightarrow a \in (p)$ or $b \in (p)$, i.e.,

$p \mid a$ or $p \mid b$, hence p is prime.

(ii) $\Rightarrow$ Suppose p is an irreducible element and (0) is any principal ideal for which $(p) \subsetneq (a) \subseteq R$. As $p \in (a)$, then we have $p = ra$ for some $r \in R$. But p is an irreducible $\Rightarrow$ either r or a is invertible, suppose r is invertible, therefore $a = r^{-1}p \in (p) \Rightarrow (a) \subseteq (p) = (a)$, which is a contradiction. Hence, a is invertible, whence $(a) = R$. Thus (p) is a maximal principal ideal.

$\Leftarrow$ Let (p) be a maximal principal ideal of R. Assume that p is not an irreducible element. Then $p = ab$, where $a, b \in R$ and neither a nor b is invertible. Now if $a \in (p)$, then $a = rp$ for some $r \in R$, hence, $p = ab = rpb$. Therefore $1 = rb$. Therefore b is invertible. Hence $a \notin (p) \Rightarrow (p) \subset (a)$. Observe that if $(a) = R$, then a will possess an inverse, contrary to assumption. We conclude, that $(p) \subset (a) \subset R$, which denies that (p) is a maximal principal ideal. Our original supposition is false and a must be an irreducible element of R.

(iii) Suppose that $p = ab$ for some $a, b \in R$. Since p is prime, either $p \mid a$ or $p \mid b$; say p divides b, so that there exists some element $c \in R$ for which $b = pc$. Then we have

$abc = pc = b \Rightarrow ac = 1$. Hence a is invertible. Hence p must be an irreducible element of R.

1.6.6 Definition: A ring R is called a principal ideal domain if

(i) it is an integral domain

(ii) every ideal is principal.

1.6.7 Theorem: Let R be a principal ideal domain and p be a non-zero element of R. Then

(i) p is a prime element iff p is irreducible.

(ii) (p) is a prime ideal iff it is maximal.

Proof: $\Rightarrow$ This follows from 1.6.5 (ii).

$\Leftarrow$ Suppose p is an irreducible element and, p divides the product ab, say $pc = ab$, with $c \in R$. As R is a principal ideal domain, the ideal generated by p and a, $(p, a) = (d)$ for some choice of d in R; hence, $p = rd$, for a suitable $r \in R$. But p is irreducible by hypothesis, so that either r or d must be an invertible element. If d happens to possess an inverse, we would have $(p, a) = R$. Thus, there would exist elements $s, t \in R$ for which $1 = sp + ta$. Then $b = b1 = bsp + bta = bsp + pct = p(bs + ct)$, which implies that $p \mid b$.

On the other hand, if r is a unit in R, then $d = r^{-1}p \in (p)$, whence $(d) \subseteq (p)$. Hence $a \in (p)$ and $P \mid a$. If $p \mid ab$, then p must divide one of the factors, so p is a prime element of R.

(ii) Since (p) is prime ideal $\Leftrightarrow$ p is prime element by 1.6.5 (i) $\Leftrightarrow$ p is irreducible by 1.6.7 (i). $\Leftrightarrow$ (p) is maximal by 1.6.5 (ii).

1.6.8 Definition: Let $a_1, a_2, \ldots, a_n \in R$, then an element d of R is called a greatest common divisor (GCD) of $a_1 \ldots a_n$ if

(i) $d \mid a_i$ for each i,

(ii) if $c \mid a_i$ for each i $\Leftrightarrow c \mid d$.

Remark: If d and d' are GCD of $a_1 \ldots a_n$ then by (ii) above $d \mid d'$ and $d' \mid d$. Hence they are associates, therefore a GCD is determined up to associates.

1.6.9 Definition: We say $a_1 \ldots a_n$ are relatively prime if their GCD is equal to 1.

1.6.10 Theorem: Let $d, a_1, \ldots, a_n \in R$, then the following conditions are equivalent:

(i) d is a GCD of $a_1, \ldots, a_n$, and $d = r_1a_1 + \ldots + r_na_n$ for $r_i \in R$

(ii) $(a_1, \ldots, a_n) = (d)$.

Proof: (ii) $\Rightarrow$ (i). Since each $a_i \in (d)$; there exist elements $b_i \in R$ for which $a_i = b_id$, whence $d \mid a_i$ for $i = 1, 2, \ldots, n$. Hence d is a common divisor of a_i. It remains only to establish that any common divisor c of the a_i also divides d.

Since $(a_1, \ldots, a_n) = (d)$, $d = x_1a_1 + \ldots + x_na_n$ for some $x_i \in R$, $i = 1, 2, \ldots, n$. Now $c \mid a_i \Rightarrow c \mid x_1a_1 + \ldots + x_na_n = d$. Hence d is a GCD of $\{a_1, \ldots, a_n\}$.

(i) $\Rightarrow$ (ii) Suppose $d = \text{GCD } \{a_1, \ldots, a_n\}$ and $d = r_1a_1 + \ldots + r_na_n$, with $r_i \in R$. Then d lies in the ideal $(a_1, \ldots, a_n) \Rightarrow (d) \subseteq (a_1, \ldots, a_n)$. Since $d = \text{GCD } \{a_1, \ldots, a_n\}$, each a_i is a multiple of d; say $a_i = x_id$, where $x_i \in R$. Thus for an arbitrary member $y_1a_1 + \ldots + y_n a_n$ of the ideal $(a_1, \ldots, a_n)$, we have

$$y_1a_1 + \ldots + y_n a_n = (y_1x_1 + \ldots + y_n x_n)\, d \in (d).$$

Hence $(a_1, \ldots, a_n) \subseteq (d)$, so

$$(a_1, \ldots, a_n) = (d).$$

1.6.11. Corollary (Bezout theorem): In a principal ideal domain every finite collection of elements $a_1, \ldots, a_n \in R$ always has a GCD = d, and $d = r_1a_1 + r_2a_2 + \ldots + r_n a_n$, where $r_i \in R$.

Proof: Since the ring is a principal ideal domain $(a_1, \ldots, a_n) = (d)$ for some $d \in R$. Then the result follows from Theorem 1.6.10.

1.6.12 Corollary: In a principal ideal domain, $a_1, \ldots, a_n \in R$ are relatively prime iff there exists $r_1, \ldots, r_n \in R$ such that

$$1 = r_1a_1 + \ldots + r_n a_n.$$

Proof: Let $a_1, \ldots, a_n \in R$. $a_1, \ldots, a_n$ are relatively prime iff GCD of them = 1, so $1 = r_1a_1 + \ldots + r_na_n$ for $r_i \in R$ by 1.6.11.

1.6.13 Corollary: Let a and b be relatively prime elements of a principal ideal domain R, then

(i) $a \mid bc \Rightarrow a \mid c$.

(ii) $a \mid c$ and $b \mid c \Rightarrow ab \mid c$.

Proof: (i) Since a and b are relatively prime then $\lambda a + \mu b = 1$. Multiplying this relation by c we obtain $\lambda ac + \mu bc = c$. Now $a \mid \lambda ac$, always and $a \mid \mu bc$, for $a \mid bc$ by assumption. Therefore $a \mid \lambda ac + \mu bc = c$.

(ii) Let $a \mid c$ and $b \mid c$, then there are r_1 and $r_2 \in R$ such that $c = ar_1$, $c = br_2$.

Hence $cb = abr_1$ and $ca = abr_2$.

There exist α, β in R such that

$$\alpha a + \beta b = 1. \quad \Rightarrow \quad \alpha ac + \beta bc = c .$$

Hence $\alpha abr_2 + \beta abr_1 = c$,

or $ab(\alpha r_2 + \beta r_1) = c$.

Hence $ab \mid c$.

1.6.14 Theorem: In a principal ideal domain every non-zero non-unit element is a product of prime elements.

Proof: We consider $X = \{(z) \mid z$ is a non-zero non-unit element of R and z is not a product of prime elements$\}$. We want to show X is empty. Suppose on the contrary X is not empty. By 1.5.5, R is noetherian, therefore X has a maximal element say (m). m is

not a prime element, therefore, by 1.6.7 (i) m is not irreducible. Therefore $m = uv$ where neither u nor v are units. Consider (u) and (v). We have $(m) \subset (u)$ and $(m) \subset (v)$. Because of the maximality of (m), (u) and $(v) \notin X$. Therefore u and v are products of prime elements. Therefore m is a product of prime elements. Then $(m) \notin X$; which is a contradiction. Hence X must be empty.

1.6.15 Definition: Let R be an integral domain, then R is called a unique factorization domain (UFD).

(i) Every non-zero non-unit a is a product of irreducible elements $q_1, q_2, \ldots, q_r \in R$.

(ii) The above representation in (i) of the element a is unique up to the order of the elements and multiplication by units, i.e., if $p_1 \ldots p_r$ and $q_1 \ldots q_s$ are two factorizations of the same element of R into irreducible elements, then $r = s$ and the q_i's can be renumbered so that p_i and q_i are associates for every i.

1.6.16 Theorem: Every principal ideal domain is a UFD.

Proof: We have already shown in 1.6.14 that over a principal ideal domain, every non-zero non-unit is a product of prime elements, i.e., irreducible elements. Now we shall show that this product representation has the uniqueness properties demanded in 1.6.15 (ii).

Let a be a non-zero non-unit and $a = p_1 \dots p_k = q_1 \dots q_\ell$ where p_i, q_j are irreducible elements. Without loss of generality, we suppose $k \leq \ell$. Now $p_1 \mid q_1 \dots q_\ell$ and p_1 is irreducible. Hence p_1 is a prime element by 1.6.7 (i), so $p_1 \mid q_j$. Let us call $q_{\pi(1)}$ for this q_j. Therefore $q_{\pi(1)} = \varepsilon_1 p_1$, but $q_{\pi(1)}$ is irreducible, therefore ε_1 is a unit or p_1 is a unit. Since p_1 is prime, then ε_1 must be a unit, so they are associates of each other. Applying this k times, we have $a = p_1 \dots p_k = \varepsilon_1\varepsilon_2 \dots \varepsilon_k \cdot q_{\pi(1)} \dots q_{\pi(k)} \cdot t$ where t is the product of the remaining q_i's if $\ell > k$, and $p_i = \varepsilon_i q_{\pi(i)}$ where ε_i is a unit. Since R is an integral domain, after cancelling the common factors we have $1 = t$. Therefore ℓ must be equal to k, and the uniqueness of the factorization follows.

1.6.17 Definition: An integral domain R is called a Euclidean domain if there exists a map $\delta : R\setminus\{0\} \longrightarrow Z^+$ with the following properties:

(1) $\delta(a) > d(0)$ for all $0 \neq a \in R$;

(2) given $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $\delta(r) < \delta(b)$.

1.6.18 Examples: Following are some examples of Euclidean domain:

(i) Let $R = Z$ with $\delta(m) = |m|^k$ for $k \in Z^+$.

(ii) Let K be a field with $\delta(x) = 1$ for all non-zero X.

(iii) Let $R = Z[i]$ (ring of Gaussian integers), with $\delta(x + yi) = x^2 + y^2$.

1.6.19 Theorem: Every Euclidean domain is a principal ideal domain.

Proof: Let R be a Euclidean domain and $\mathcal{A}$ an ideal in R. If $\mathcal{A}$ is the zero ideal, then $\mathcal{A} = (0)$ and so is principal. Otherwise consider the non-emtpy subset X of Z given by $X = \{\delta(a) \mid a \in \mathcal{A},\ a \neq 0\}$. By property (1) of the function δ, $x > \delta(0)$ for all $x \in X$. Thus X is a non-empty subset of Z which is bounded from below. Hence X has a minimal element. Let $0 \neq b \in \mathcal{A}$ be such that $d(b)$ is a minimal element of X. We want to show that $\mathcal{A} = (b)$.

Suppose $a \in \mathcal{A}$. Then there exist elements q and r in R such that $a = qb + r$ with $\delta(r) < \delta(b)$. Since $a \in \mathcal{A}$, $qb \in \mathcal{A}$, we have $r = a - qb \in \mathcal{A}$. But $\delta(r) < \delta(b)$, which contradicts the choice of b unless $r = 0$. Hence $a = qb$ and $\mathcal{A} = (b)$. Therefore every ideal of R is principal.

1.6.20 Corollary: Every Euclidean ring is a UFD.

Remark: Note the following implications:

1. Every Euclidean domain is a principal ideal domain and every principal ideal domain is a unique factorization domain.
2. None of these implications are reversible.

There exists an algorithm to determine the GCD of two elements a_1, a_2 in a Euclidean domain. This is called the Euclidean algorithm, which is explained below:

Given $a_1, a_2 \in R$. Without loss of generality, we suppose $\delta(a_2) \leq \delta(a_1)$. Then

$$a_1 = q_1 a_2 + a_3 \quad \text{with} \quad a_3 = 0 \quad \text{or} \quad \delta(a_3) < \delta(a_2) \quad \text{if} \quad a_3 \neq 0$$

$$a_2 = q_2 a_3 + a_4 \quad \text{with} \quad a_4 = 0 \quad \text{or} \quad \delta(a_4) < \delta(a_3) \quad \text{if} \quad a_4 \neq 0$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$a_{n-1} = q_{n-1} a_n + a_{n+1} \quad \text{with} \quad a_{n+1} = 0 \quad \text{or} \quad \delta(a_{n+1}) < \delta(a_n) \quad \text{if} \quad a_{n+1} \neq 0$$

$$a_n = q_n a_{n+1} + a_{n+2} \quad \text{with} \quad a_{n+2} = 0 . \quad (\text{but } a_{n+1} \neq 0) .$$

Then $d = a_{n+1}$ is the GCD of a_1, a_2. From the last equation $d \mid a_n$, and by using the previous equation we find $d \mid a_{n-1}$, $d \mid a_{n-2}, \ldots, d \mid a_2, d \mid a_1$. Hence d is a common divisor of a_1 and a_2. Suppose $c \mid a_1$ and $c \mid a_2$, then $c \mid a_3$, $c \mid a_4, \ldots, c \mid a_{n+1} = d$.

The above algorithm can be expressed neatly in a matrix form. We have for any i the equation

$$a_i = q_i a_{i+1} + a_{i+2} .$$

Take the form

$$\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{i+1} \\ a_{i+2} \end{pmatrix} = \begin{pmatrix} a_i \\ a_{i+1} \end{pmatrix}, \quad n \geq i \geq 1 .$$

Suppose

$$A = \prod_{i}^{n} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{then} \quad A \begin{pmatrix} a_{n+1} \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} .$$

Note that A is invertible, and so we can write

$$\begin{pmatrix} a_{n+1} \\ \vdots \\ 0 \end{pmatrix} = A^{-1} \begin{pmatrix} a_1 \\ \\ a_2 \end{pmatrix}, \quad \text{and therefore} \quad (a_1, a_2) = (a_{n+1}).$$

1.7 Modules

We now define a module, a basis of a module and a free module.

1.7.1 Definition: Let R be a ring. An R-module is an additive abelian group M together with a function $R \times M \to M$ such that for all $r,s \in R$ and $a,b \in M$

(i) $r(a + b) = ra + rb$,

(ii) $(r + s)a = ra + sa$,

(iii) $r(sa) = (rs)a$.

If R has an identity element 1_R and

(iv) $1_R a = a$ for all $a \in M$,

then M is said to be a unitary R-module.

For us, the most important R-modules will be the n-tuple modules R^n, where R^n denotes the R-module $R \oplus R \oplus \ldots \oplus R$ (n summands), for R is itself an R-module.

1.7.2 Definition: A subset X of an R-module M is said to be linearly independent provided that for distinct $x_1, \ldots, x_n \in X$ and $r_i \in R$.

$$r_1x_1 + r_2x_2 + \ldots + r_nx_n = 0 \Longrightarrow r_i = 0 \quad \text{for every } i .$$

A set that is not linearly independent is said to be linearly dependent.

1.7.3 Definition: A basis $\mathcal{B}$ of a module M is a linearly independent subset which spans (or generates) the module.

The important property of a basis $\mathcal{B}$ is that each element of $\mathcal{B}$ can be expressed uniquely as a linear combination of (some finite numbers of) elements of $\mathcal{B}$.

1.7.4 Definition: An R-module M is called a free module if it has a basis. If M has a finite basis containing n elements, then M is called a free R-module with n generators.

It can be shown that a free R-module is isomorphic to a direct sum of copies of R. In particular, a free R-module with n generators is isomorphic to R^n.

1.8 Bezout Domain

1.8.1 Definition: A ring R is called a Bezout Domain if the sum of two principal ideals is principal.

Remarks: (i) Clearly every principal ideal domain is a Bezout domain.

(ii) In a Bezout domain any two elements have a GCD.

More precisely

1.8.2 Theorem [C, Page 277]: (i) A Bezout domain has the following property (B); any two elements a, b have a GCD d and there exist r_1 and r_2 such that

$$d = ar_1 + br_2 .$$

Conversely, any integral domain with this property (B) is Bezout domain.

(ii) Moreover, in a Bezout domain R any finitely generated ideal is principal, more precisely,

$$(a_1, \ldots, a_n) = (d) \quad , \text{ where } d \text{ is a GCD of } a_1, \ldots, a_n .$$

Thus any finite set of elements of R has a GCD.

Proof: Suppose R is a Bezout domain, hence R is an integral domain in which any ideal generated by two elements, is principal.

Now, let $a, b \in R$, then the ideal generated by a and b is principal, say

$$(a, b) = (d) \qquad \text{------ (1)}$$

This means that,

$$d = ar_1 + br_2 \qquad \text{-----} \quad (2)$$

and

$$a = da_1 \ , \quad b = db_1 \qquad \text{-----} \quad (3)$$

We exclude the trivial case where $a = 0$ or $b = 0$. (3) implies d is a common factor of a and b. Now (2) shows that, any common factor of a and b is also a factor of d; thus d is indeed a GCD of a and b. Conversely, suppose R be an integral domain with the property (B) as in the statement of the theorem.

We want to show R is a Bezout domain.

Let $a, b \in R$. We exclude the trivial case $a = 0$ or $b = 0$. By property (B) there exist a $d \in R$ such that d is GCD of a and b and

$$d = ar_1 + br_2 \text{ for some } r_1 , r_2 \in R \qquad \text{-----} \quad (4)$$

Hence, $d \mid a$, $d \mid b$ i.e., $a = da_1$, $b = db_1$ ----- (5)

for some $a_1, b_1 \in R$.

We claim $(a, b) = (d)$

by (4) $d \in (a, b)$ therefore $(d) \subseteq (a, b)$

by (5) $a \in (d)$, $b \in (d)$ therefore $(a, b) \subseteq (d)$

Hence $(a, b) = (d)$.

(ii) For the last paragraph.

We first show, by induction on n, that every ideal generated by n elements is principal. For $n = 1$ there is nothing to prove and for $n = 2$ this is true by definition. Now let $n > 2$ and assume that every ideal on $n-1$ generators is principal.

Given $a_1, \ldots, a_n \in R$.

$$(a_1, a_2, \ldots, a_n) = (a_1, (a_2, \ldots, a_n))$$
$$= (a_1, (b))$$

where by induction

$$(a_2, \ldots, a_n) = (b)$$

therefore, $(a_1, a_2, \ldots, a_n) = (a_1, b)$
$$= (d)$$

by induction hypothesis for $n = 2$.

Given $a_1, \ldots, a_n$, not all zero, let

$$d = \sum a_i b_i \qquad \text{-----} \quad (6)$$

and

$$a_i = da_i \quad (i = 1, \ldots, n) \qquad \text{-----} \quad (7)$$

By (7), d is common factor of $a_1, \ldots, a_n$ and by (6), any common factor of the a_i is a factor of d, so d is a GCD of $a_1, \ldots, a_n$.

Remark: A commutative ring (not necessarily domain) is called an F-ring if all finitely generated ideals are principal. Hence an F-domain is the same as the Bezout domain. F-rings have been introduced and studied by Gillman and Henriksen ([G-H]$_2$).

Most of the F-rings known are rings of continuous functions over suitable topological spaces since these considerations depend very heavily on topology, we will not consider them in detail. The interested reader may refer [G-H]$_2$).

Another important example of a Bezout domain is the ring of entire functions. For details please refer [H]$_2$.

However, we present here an example of a Bezout domain, which is not a principal ideal domain.

1.8.3 Example: Let R be the ring of polynomials over Q, with the constant term an integer.

$$R = \{f \mid f \in Q[X] \ , \ f(0) \in Z\}$$

We claim this is not a principal ideal domain, but a Bezout domain.

First we show that R is a Bezout domain.

Let $f, g \in R$. Without loss of generality, we may assume f and g have no common factor of positive degree in X, and no common factor either.

Now, $f, g \in Q[X]$ which is a principal ideal domain. Hence there exist $u, v \in Q[X]$ such that

$$fu - gv = 1 \quad \text{---} \quad \begin{cases} u(0) = p/q \\ v(0) = r/s \end{cases}$$

where p, q, r and s are integers. By multiplying by a suitable integer, we may assume that

$$u, v \in R \text{ and } fu - gv = \gamma , \quad \gamma \in Z$$

Let $f(0) = \alpha$, $g(0) = \beta$, $\alpha, \beta \in Z$

$$f = \alpha + f_1 , \quad g = \beta + g_1$$

where $f_1(0) = g_1(0) = 0$, so $f_1, g_1 \in R$

Now, $\alpha = f - (\frac{f_1}{\gamma})$ where $\frac{f_1}{\gamma} \in R$

$$= f - (\frac{f_1}{\gamma})(fu - gv)$$

$$= (1 - \frac{f_1}{\gamma} \cdot u) f + (\frac{f_1}{\gamma} \cdot v) g .$$

But $(1 - \frac{f_1}{\gamma} \cdot u) \in R \Rightarrow (1 - \frac{f_1}{\gamma} \cdot u) f \in fR$

$(\frac{f_1}{\gamma} \cdot v) \in R \Rightarrow (\frac{f_1}{\gamma} \cdot v) g \in gR .$

Hence $\alpha \in fR + gR .$

Similarly $\beta \in fR + gR.$

Now $f(0)\, u\,(0) - g(0)\, v(0) = \alpha u(0) - \beta v(0) = \gamma$

Let $\delta = (\alpha, \beta)$. Now $\delta \mid \alpha$, $\delta \mid \beta$, whence $\delta \mid \gamma$.

This implies $\delta \mid \alpha + (\frac{f_1}{\gamma})\gamma = f$

Similarly $\delta \mid g$.

Hence $fR \subseteq \delta R$ and $gR \subseteq \delta R$,

so, $fR + gR \subseteq \delta R$.

Now, $\delta = \alpha x + \beta y$, $x \in Z$, $y \in Z$

$\in x\ (fR + gR) + y\ (fR + gR)$

$\in fR + gR$.

Hence $\delta R \subseteq fR + gR$.

Therefore $fR + gR = \delta R$.

Now we want to show that R is not a principal ideal domain.

Consider the ideal I generated by $\{\frac{X}{2}, \frac{X}{2^2}, \frac{X}{2^3}, \ldots\}$

We claim I is not a principal ideal.

Let $(f) = (\frac{X}{2}, \frac{X}{2^2}, \ldots, \frac{X}{2^n}, \ldots) = I$

we then have

$$\frac{X}{2^i} = f\, g_i \quad \text{where} \quad g_i \in R \qquad \text{-----} \quad (1)$$

there exist $f = \sum_{j=1}^{m} h_j \frac{X}{2^j}$ ----- (2)

Let $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$

$g = b_{i_0} + b_{i_1}X + b_{i_2}X^2 + \ldots + b_{i_{\ell_i}}X^{\ell_i}$

Since $f \cdot g_i = \frac{X}{2^i}$ we have $\begin{cases} a_i = 0 & \text{for } i > 1 \\ b_{i_k} = 0 & \text{for } k > 1 \end{cases}$

so $f = a_0 + a_1 X$

$g_i = b_{i_0} + b_{i_1} X$

hence $f \cdot g_i = a_0 b_{i_0} + (a_0 b_{i_1} + a_1 b_{i_0}) X + a_1 b_{i_1} X^2 = \frac{X}{2^i}$

hence $a_0 b_{i_0} = 0 = a_1 b_{i_1}$.

On the other hand by equation (2)

$$f(0) = a_0 = \sum_{j=1}^{m} h_j(0) \frac{0}{2^j} = 0$$

hence $f(X) = a_1 X$.

Now $a_1 \neq 0$, otherwise $f = 0$ which is a contradiction,

hence in g_i, $b_{i_1} = 0$.

We have finally $f = a_1 X$ and $g_i = b_{i_0}$, and (1) becomes

$$f \cdot g_i = a_1 X \cdot b_{i_0} = \frac{X}{2^i}$$

and $a_1 \in Q$, but $b_{i_0} \in Z$

Therefore, let $a_1 = \frac{u}{v}$ where $u, v \in Z$ and u and v are relatively prime. Therefore

$$\frac{u}{v} \cdot b_{i_0} = \frac{1}{2^i}$$

(*) $2^i u \cdot b_{i_0} = v$ true for all i?

As i increases b_{i_0} must decrease since v is a constant, yet b_{i_0} must remain an integer which is impossible, hence (*) not true. So no such f exists.

CHAPTER II

Elementary linear algebra over a commutative ring with identity

In this chapter, we shall discuss some of the elementary properties of matrices and investigate the closely related theory of determinants. R shall always denote a commutative ring with identity, unless otherwise stated.

2.1 Matrices

2.1.1 Definition: An array of elements of the form

$$\begin{pmatrix} a_{11} & a_{12} & a_{1m} \\ a_{21} & a_{22} & a_{2m} \\ \vdots & & \vdots \\ a_{n1} & a_{n2}\cdots & a_{nm} \end{pmatrix}$$

where $a_{ij} \in R$ with n rows and m columns is called an $n \times m$ matrix over R.

Since a matrix is in general a two dimensional array of elements, a double subscript must be used to represent any one of its elements.

Remarks: (i) Any matrix which has the same number of rows as columns is called a square matrix.

(ii) An arbitrary matrix is usually denoted by a capital letter (A, B, C, etc.) or by $((a_{ij}), (b_{ij})$, etc.), which indicates

that the $(i, j)^{th}$ entry is element $a_{ij} \in R$, for $i = 1, \ldots, n$ and $j = 1, \ldots, m$.

2.1.2 Definition: If in an $n \times m$ matrix A, $n = 1$, we call the matrix A, a row matrix, and if $m = 1$, then we call the matrix A, a column matrix. The entries $a_{11}, a_{22}, \ldots, a_{nn}$ (if $n < m$) or $a_{11}, \ldots, a_{mm}$ (if $m < n$) is called the principal diagonal.

2.1.3 Definition: Two matrices A and B are said to be equal, written $A = B$, if they are identical, that is, if the corresponding elements are equal. Thus two $n \times m$ matrices (a_{ij}) and (b_{ij}) are equal if and only if $a_{ij} = b_{ij}$ in R for all i, j.

2.1.4 Definition: The matrix A is called lower triangular if all the entries above the main diagonal are zeros, i.e., iff $a_{ij} = 0$ for $i < j$. Similarly if all the entries below the main diagonal are zeros, it is called upper triangular, i.e., iff $a_{ij} = 0$ for $j < i$. A is called strictly upper triangular iff $a_{ij} = 0$ for $j \leq i$.

2.1.5 Definition: An $n \times n$ matrix (a_{ij}) with $a_{ij} = 0$ for all $i \neq j$ is called a diagonal matrix.

2.1.6 Definition: If R has an identity element, the identity matrix I_n is a square matrix having once along the main diagonal (the diagonal running from upper left to lower right) and zero elsewhere. If we write $I_n = (\delta_{ij})$, then

$$\delta_{ij} = \begin{cases} 1 & , \quad i = j \\ 0 & , \quad i \neq j \end{cases} \qquad \ldots \quad (1)$$

The symbol δ_{ij}, defined by (1) is called the Kronecker delta. This symbol will always refer to the Kronecker delta unless otherwise specified.

2.1.7 Definition: A matrix whose elements are all zero is called a null or zero matrix and is denoted by 0.

A null matrix does not need to be square.

2.1.8 Definitions: (i) The transpose of $n \times m$ matrix $A = (a_{ij})$ is an $m \times n$ matrix (b_{ij}) formed from A by interchanging rows and columns such that row (column) i of A becomes column (row) i of the transposed matrix, (b_{ij}), i.e., $b_{ij} = a_{ji}$ for all i, j. The transpose is denoted by A^t.

(ii) If $A = A^t$, then we say A is symmetric (note it is a square matrix), i.e., A is symmetric if $a_{ij} = a_{ji}$.

(iii) If $A = -A^t$, then A is called skew-symmetric (antisymmetric), i.e., A is skew-symmetric iff $a_{ij} = -a_{ji}$ for all i, j.

A skew-symmetric matrix is a square matrix with diagonal elements zero, i.e., $a_{ii} = 0$ for all i (if R is not of characteristic 2).

2.2 Matrix addition and multiplication

2.2.1 Definition: Given an $n \times m$ matrix $A = (a_{ij})$ and $\lambda \in R$, the product of λ and A, written λA is the $n \times m$ matrix (λa_{ij}). (We note that $\lambda A = (\lambda a_{ij}) = (a_{ij}\ \lambda) = A\lambda$.) λI_n is called a scalar matrix.

2.2.2 Definition: If $A = (a_{ij})$ and $B = (b_{ij})$ are two matrices having the same number of rows and columns, say $n \times m$ matrices, then, the sum $A + B$ is defined to be the $n \times m$ matrix (c_{ij}), where

$$c_{ij} = a_{ij} + b_{ij}.$$

Note that addition of matrices A, B is defined only when B has the same number of rows and the same number of columns as A.

Subtraction is defined in terms of operations already considered:

$$A - B = A + (-1)B.$$

2.2.3 Definition: If $A = (a_{ij})$ is an $m \times p$ matrix and $B = (b_{ij})$ is a $p \times q$ matrix then the product AB is defined to be the $m \times q$ matrix (c_{ij}), where $c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}$ $\quad i = 1, \ldots, m$ and $j = 1, \ldots, q$.

Remarks: (i) Multiplication is not commutative in general.

(ii) If the matrix product AB is defined, then so is the product $B^t A^t$ of transpose matrices.

2.2.4 Lemma: If A, B are two matrices such that the sum $A + B$ and the product AB are defined, then

(i) $(A^t)^t = A$,

(ii) $(A + B)^t = A^t + B^t$,

(iii) $(\lambda A)^t = \lambda A^t$ for λ is scalar,

(iv) $(AB)^t = B^t A^t$.

Proof: The proofs of parts (i), (ii) and (iii) are straightforward; we content ourselves with proving part (iv).

Suppose that $A = (a_{ij})$ and $B = (b_{ij})$, then $AB = (c_{ij})$, where $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. Therefore, by definition, $(AB)^t = (\lambda_{ij})$, where $\lambda_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk} b_{ki}$. On the other hand, $A^t = (\mu_{ij})$ where $\mu_{ij} = a_{ji}$ and $B^t = (\gamma_{ij})$ where $\gamma_{ij} = b_{ji}$, whence the (i, j) element of $B^t A^t$ is $\sum_{k=1}^{n} \gamma_{ik} \mu_{kj} = \sum_{k=1}^{n} b_{ki} a_{jk} = \sum_{k=1}^{n} a_{jk} b_{ki} = \lambda_{ij}$. Thus

$$(AB)^t = B^t A^t .$$

Remark: The same result as in 2.2.4 (iv) holds for any finite number of factors, i.e.,

$$(A_1 A_2 \ldots A_n)^t = A_n^t \ldots A_2^t A_1^t .$$

2.2.5 Theorem: For each integer $n \geq 1$ and any ring R, the set $M_n(R)$ of all $n \times n$ matrices is a ring.

Proof: See 1.1.5 (iii).

2.3 Equivalent and Elementary Matrices

2.3.1 Definition: A matrix $A \in Mat_n R$ is said to be invertible or non-singular if there exists $B \in Mat_n R$ such that $AB = I = BA$.

Remark: The inverse matrix B, if it exists, is easily seen to be unique; it is usually denoted by A^{-1}. Clearly $B = A^{-1}$ is invertible and $(A^{-1})^{-1} = A$. The product AC of two invertible matrices is invertible with $(AC)^{-1} = C^{-1}A^{-1}$. If A is an invertible matrix over a commutative ring, then so is its transpose and $(A^t)^{-1} = (A^{-1})^t$.

2.3.2 Definition: Two matrices $A, B \in Mat_n R$ are said to be similar if there exists an invertible matrix P such that $B = PAP^{-1}$. Two $n \times m$ matrices, C, D are said to be equivalent if there exist invertible matrices P and Q such that $D = PCQ$.

Remarks: (i) If A and B are similar, then they are equivalent.

(ii) We shall frequently consider the rows (resp. columns) of a given $n \times m$ matrix over a ring R as being elements of R^m[resp. R^n]. We shall speak of adding a scalar multiple of one row [resp. column] to another; for example,

$$r(a_1, a_2, \ldots, a_m) + (b_1, b_2, \ldots, b_m) =$$

$$(ra_1 + b_1, \ldots, ra_m + b_m).$$

2.3.3 Definition: Let A be a matrix over a ring R with identity. Each of the following is called an elementary row operation on A:

(i) interchange two rows of A;

(ii) multiply a row of A by a unit $c \in R$;

(iii) for $r \in R$ and $i \neq j$, add r times row j to row i.

Remarks: (i) Elementary column operations on A are defined analogously.

(ii) All these operations are reversible or rather invertible. Given an elementary operation T, the operation T', which reverses T is unique and is called the inverse of T.

2.3.4 Definition: An $n \times n$ elementary matrix is a matrix that is obtained by performing exactly one elementary row (or column) operation on the identity matrix I_n.

2.3.5 Theorem: Let A be an $n \times m$ matrix over a ring R with identity, T an elementary row operation on I_n, and E_n the elementary matrix obtained by performing T. Then E_nA = the matrix obtained by performing the operation T on A.

Proof: Let ρ^i be the ith row of A; we denote this by writing $A = \begin{pmatrix} \rho^1 \\ \vdots \\ \rho^n \end{pmatrix}$. If B is a matrix for which AB is defined, then $AB = \begin{pmatrix} \rho^1 B \\ \vdots \\ \rho^n B \end{pmatrix}$. Let ε_i be the $1 \times n$ matrix whose kth entry $= \delta_{ik}$,

then clearly $e_iA = \sum \delta_{ik}\rho^i = \rho^i$. We also remark that $I_n = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$ is the identity matrix.

(i) Let T be the elementary row operation $\rho^i \leftarrow \rho^j$. Then $E_n = T(I_n)$ is the matrix whose ith row is e_j and jth row is e_i and the rest of the rows are the same as that of I_n. Similarly $T(A)$ is the matrix obtained from A by interchanging ith and jth rows. Thus

$$E_nA = \begin{pmatrix} e_1A \\ \vdots \\ e_jA \\ \vdots \\ e_iA \\ \vdots \\ e_nA \end{pmatrix} = \begin{pmatrix} \rho^1 \\ \vdots \\ \rho^j \\ \vdots \\ \rho^i \\ \vdots \\ \rho^n \end{pmatrix} = T(A).$$

(ii) Now, let T be the elementary row operation $\rho^i \to c\rho^i$, $c \neq 0$, c is invertible. Then

$$E_n = T(I) = \begin{pmatrix} e_1 \\ \vdots \\ ce_i \\ \vdots \\ e_n \end{pmatrix} \quad \text{and}$$

$$T(A) = \begin{pmatrix} \rho^1 \\ \vdots \\ c\rho^i \\ \vdots \\ \rho^n \end{pmatrix}, \quad \text{thus}$$

$$E_n A = \begin{pmatrix} e_1 A \\ \vdots \\ ce_i A \\ \vdots \\ e_n A \end{pmatrix} = \begin{pmatrix} \rho' \\ \vdots \\ c\rho^i \\ \vdots \\ \rho^n \end{pmatrix} = T(A)$$

(iii) Lastly, let T be the elementary row operation $\rho^i \to k\rho^j + \rho^i$.

Then,

$$E_n = T(I) = \begin{pmatrix} e_1 \\ \vdots \\ ke_j + e_i \\ \vdots \\ e_m \end{pmatrix} \quad \text{and}$$

$$T(A) = \begin{pmatrix} \rho' \\ \vdots \\ k\rho^j + \rho^i \\ \vdots \\ \rho^m \end{pmatrix}$$

Using $(ke_j + e_i)\, A = ke_jA + e_iA = kR^j + R^i$, we have

$$E_n A = \begin{pmatrix} e_1 A \\ \vdots \\ (ke_j + e_i)A \\ \vdots \\ e_m A \end{pmatrix}$$

$$= \begin{pmatrix} \rho' \\ \vdots \\ k\rho^j + \rho^i \\ \vdots \\ \rho^m \end{pmatrix}$$

$$= T(A).$$

Thus we have proved the theorem.

Remark: Let A be an $n \times m$ matrix over a ring R with identity and let E_m be the elementary matrix obtained by performing an elementary column operation T on I_m. Then AE_m is the matrix obtained by performing the operation T on A.

Proof: Similar to 2.3.5.

2.3.6 Corollary: Every $n \times n$ elementary matrix E over a ring R with identity is invertible and its inverse is an elementary matrix.

Proof: Let E be the elementary matrix corresponding to the elementary row operation T; $T(I) = E$. Let T' be the inverse operation of T, and F be its corresponding elementary matrix. Then by 2.3.5

$$I = T'(T(I)) = T'E = FE \quad \text{and}$$
$$I = T(T'(I)) = TE' = EF' \quad \text{and}$$

Therefore F' is the inverse of E.

2.3.7 Corollary: If B is the matrix obtained from an $n \times m$ matrix A over a ring R with identity be performing a finite sequence of elementary row and colum operations, then B is equivalent to A.

Proof: Since each row [column] operation used to obtain B from A is given by left [right] multiplication by an appropriate

elementary matrix (theorem 2.3.5, we have $B = (E_p \dots E_1)A(F_1 \dots F_q) = PAQ$ with each E_iE_j an elementary matrix and $P = E_p \dots E_1$, $Q = F_1 \dots F_q$, P and G are products of invertible matrices by 2.3.6, and so they are themselves invertible.

2.4 Determinants

In order to define and study determinants we shall need the notion of a permutation and its properties, which we present below.

Let $S = \{1, 2, \dots, n\}$, and let $\rho : S \to S$ be a bijection, then ρ is called a permutation. The set S_n of all permutations on S under multiplication is a group, called the symmetric group of order n.

$$w = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \quad \text{is the identity of } S_n;$$

if $$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \text{ then } \rho^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

In general $\rho\sigma \neq \sigma\rho$.

The number $V_n = \prod_{1 \leq r < s \leq n} (s - r)$ is clearly positive; if ρ is any permutation, we define $\rho(V_n) = \prod_{1 \leq r < s \leq n} (\rho(s) - \rho(r))$. The factors in V_n and $\rho(V_n)$ are identical apart from a possible change of sign. Hence $\rho(V_n) = \operatorname{sgn} \rho \, V_n$, where $\operatorname{sgn} \rho = \pm 1$.

Example: Let $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, then $V_4 = (2-1)(3-1)(4-1)(3-2)(4-2)(4-3)$,

$$\rho(V_4) = (3-2)(4-2)(1-2)(4-3)(1-3)(1-4)$$

$$= [-(2-1)][-(3-1)][-(4-1)](3-2)(4-2)(4-3)$$

$$= -V_4 . \qquad \text{Here } \operatorname{sgn}\rho = -1.$$

$\operatorname{sgn}\rho$ is called the signature of ρ. ρ is even if $\operatorname{sgn}\rho = 1$ and is odd if $\operatorname{sgn}\rho = -1$.

$\operatorname{sgn}\rho = (-1)^k$ where k is the number of pairs r, s with $r < s$ but $\rho(r) > \rho(s)$, i.e., k is the number of inversions.

Examples: $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$, $k = 6$, $\operatorname{sgn}\rho = +1$, ρ is even.

$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}$, $k = 3$, $\operatorname{sgn}\rho = -1$, ρ is odd.

w (no inversion) $\Rightarrow \operatorname{sgn} w = 1 \Rightarrow w$ even (w is identity).

Let $\rho, \sigma \in S_n$, then

$$\operatorname{sgn}(\rho\circ\sigma) = (\operatorname{sgn}\rho)(\operatorname{sgn}\sigma).$$

For $(\rho\circ\sigma)(V_n) = \prod_{1\le r<s\le n} (\rho\circ\sigma(r) - \rho\circ\sigma(s))$

$$= \operatorname{sgn}\rho \prod_{1\le r<s\le n} (\rho(r) - \rho(s))$$

$$= (\operatorname{sgn}\sigma)(\operatorname{sgn}\rho) V_n .$$

In particular, $\operatorname{sgn} w = \operatorname{sgn}\rho\rho^{-1} = \operatorname{sgn}\rho \operatorname{sgn}\rho^{-1}$

$\Rightarrow \operatorname{sgn}\rho \operatorname{sgn}\rho^{-1} = 1$

$\Rightarrow \operatorname{sgn}\rho = \operatorname{sgn}\rho^{-1}$.

Throughout this section all rings are commutative with identity and all modules are unitary.

If B is an R-module and $n \geq 1$ an integer, B^n will denote the R-module $B \oplus B \oplus \ldots \oplus B$ (n summands). We note that the underlying set of B^n is just the cartesian product $B \times B \ldots \times B$.

2.4.1 Definition: Let $B_1, \ldots, B_n$ and C be R-modules. A function $f : B_1 \times \ldots \times B_n \to C$ is said to be R-multilinear if for each $i = 1, 2, \ldots, n$ and all $r, s \in R$, $b_j \in B_j$ and $b, b' \in B_i$:

$$f(b_1, \ldots, b_{i-1}, rb + sb', b_{i+1}, \ldots, b_n) =$$
$$rf(b_1, \ldots, b_{i-1}, b, b_{i+1}, \ldots, b_n) + sf(b_1, \ldots, b_{i-1}, b', b_{i+1}, \ldots, b_n).$$

Remark: If $C = R$, then f is called an n-linear or R-multilinear form. If $C = R$ and $B_1 = B_2 = \ldots = B_n = B$, then f is called an R-multilinear form on B.

The 2-linear functions are usually called bilinear.

2.4.2 Definitions: (i) Let B and C be R-modules and let $f : B^n \to C$ be an R-multilinear function. Then f is said to be symmetric if

$$f(b_{\sigma(1)}, \ldots, b_{\sigma(n)}) = f(b_1, \ldots, b_n)$$

for every permutation $\sigma \in S_n$.

(ii) f is said to be <u>skew-symmetric</u> if

$$f(b_{\sigma(1)}, \ldots, b_{\sigma(n)}) = (\operatorname{sgn} \sigma)\, f(b_1, \ldots, b_n)$$

for every $\sigma \in S_n$.

(iii) f is said to be <u>alternating</u> if

$$f(b_1, \ldots, b_n) = 0$$

whenever $b_i = b_j$ for some $i \neq j$.

2.4.3 <u>Example</u>: Let B be the free R-module $R \oplus R$ and let $d : B \times B \to R$ be defined by $d : ((a_{11}, a_{12}), (a_{21}, a_{22})) \to a_{11}a_{22} - a_{12}a_{21}$. Here we have $b_1 = (a_{11}, a_{12})$ and $b_2 = (a_{21}, a_{22})$, so

$$d((a_{11}\ a_{12}), (a_{21}\ a_{22})) = d(b_1, b_2) = a_{11}\ a_{22} - a_{12}\ a_{21}.$$

Then d is skew-symmetric, for

$$\begin{aligned} d(b_2, b_1) &= d((a_{21}, a_{22}), (a_{11}, a_{12})) \\ &= a_{21}\ a_{12} - a_{22}\ a_{11} \\ &= -(a_{11}\ a_{22} - a_{21}\ a_{12}) \\ &= -\,d(b_1, b_2). \end{aligned}$$

Clearly d is an alternating bilinear form on B.

2.4.4 <u>Theorem</u>: If B and C are modules over a commutative ring R with identity, then every alternating R-multilinear function $f : B^n \to C$ is skew-symmetric.

Proof: We want to show that

$$f(b_1, b_2, b_3, \ldots, b_n) = -f(b_2, b_1, b_3, \ldots, b_n) \quad \text{if} \quad \sigma = (1\ 2).$$

We have

$$\begin{aligned} 0 &= f(b_1 + b_2, b_1 + b_2, b_3, \ldots, b_n) \\ &= f(b_1, b_1+b_2, b_3, \ldots, b_n) + f(b_2, b_1+b_2, b_3, \ldots, b_n) \\ &= f(b_1, b_1, b_3, \ldots, b_n) + f(b_1, b_2, b_3, \ldots, b_n) + f(b_2, b_1, b_3, \ldots, b_n) \\ &\qquad + f(b_2, b_2, b_3, \ldots, b_n) \\ &= 0 + f(b_1, b_2, b_3, \ldots, b_n) + f(b_2, b_1, b_3, \ldots, b_n) + 0 \end{aligned}$$

whence

$$\begin{aligned} f(b_1, b_2, b_3, \ldots, b_n) &= -f(b_2, b_1, b_3, \ldots, b_n). \\ &= \operatorname{sgn} \sigma\ f(b_2, b_1, b_3, \ldots, b_n). \end{aligned}$$

Our main interest is in alternating n-linear forms on the free-R-module R^n. Such a form is a function from $(R^n)^n = R^n \oplus \ldots \oplus R^n$ (n summands) to R.

In the following discussion we have followed Hungerford [H_U].

2.4.5 Theorem: If R is a commutative ring with identity and $r \in R$, then there exists a unique alternating R-multilinear form $f:(R^n)^n \to R$ such that $f(\varepsilon_1, \ldots, \varepsilon_n) = r$, where $\{\varepsilon_1, \ldots, \varepsilon_n\}$ is the standard basis of R^n.

Remark: Since the elements of R^n may be identified with $1 \times n$ row vectors, it is clear that there is an R-module isomorphism $(R^n)^n \cong \mathrm{Mat}_n R$ given by $(X_1, X_2, \ldots, X_n) \mapsto A$, where A is the matrix with rows $X_1, X_2, \ldots, X_n$. If $\{\varepsilon_1, \ldots, \varepsilon_n\}$ is the standard basis of R^n, then $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \mapsto I_n$ under this isomorphism.

Proof of (2.4.5): (Uniqueness) If such an alternating n-linear form f exists and if $(X_1, \ldots, X_n) \in (R^n)^n$, then for each i there exist $a_{ij} \in R$ such that $X_i = (a_{i1}, a_{i2}, \ldots, a_{in}) = \sum_{j=1}^{n} a_{ij} \varepsilon_j$. Therefore by multilinearity,

$$f(X_1,\ldots,X_n) = f\Big(\sum_{j_1} a_{1j_1}\varepsilon_{j_1}, \sum_{j_2} a_{2j_2}\varepsilon_{j_2}, \ldots, \sum_{j_n} a_{nj_n}\varepsilon_{j_n}\Big)$$

$$= \sum_{j_1}\sum_{j_2}\cdots\sum_{j_n} a_{1j_1} a_{2j_2}\cdots a_{nj_n} f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n).$$

Since f is alternating the only possible nonzero terms in the final sum are those where $j_1, j_2, \ldots, j_n$ are all distinct; that is, $\{j_1, \ldots, j_n\}$ is simply the set $\{1, 2, \ldots, n\}$ in some order, so that for some permutation $\sigma \in S_n$, $(j_1, \ldots, j_n) = (\sigma_1, \ldots, \sigma_n)$. Consequently by Theorem 2.4.4:

$$f(X_1,\ldots, X_n) = \sum_{\sigma\in S_n} a_{1\sigma 1}\, a_{2\sigma 2} \cdots a_{n\sigma n}\, f(\varepsilon_{\sigma 1}, \varepsilon_{\sigma 2}, \ldots, \varepsilon_{\sigma n}).$$

$$= \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\, a_{1\sigma 1} \cdots a_{n\sigma n}\, f(\varepsilon_1, \varepsilon_2, \ldots \varepsilon_n)$$

Since $f(\varepsilon_1, \ldots, \varepsilon_n) = r$, we have

$$f(X_1, \ldots, X_n) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, r\, a_{1\sigma 1}\, a_{2\sigma 2} \cdots a_{n\sigma n}$$

$$= r \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{1\sigma 1}\, a_{2\sigma 2} \cdots a_{n\sigma n} .$$

Hence $f(X_1, \ldots, X_n)$ is uniquely determined by $X_1, \ldots, X_n$ and r.

(Existence) Define a function $f:(R^n)^n \to R$ by

$$f(X_1, X_2, \ldots, X_n) = r \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{1\sigma 1}\, a_{2\sigma 2} \cdots a_{n\sigma n} ,$$

where $X_i = (a_{i1}, \ldots, a_{in})$. To show that f is linear we show that

$$f(X_1, \ldots, \alpha X_i, \ldots, X_n) = \alpha f(X_1, \ldots, X_i, \ldots, X_n),$$

where

$$\alpha X_i = (\alpha a_{i1}, \ldots, \alpha a_{ij}, \ldots, \alpha a_{in}).$$

Now, by the definition of f

$$f(X_1, \ldots, \alpha X_i, \ldots, X_n) = r \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{1\sigma 1} \cdots (\alpha\, a_{i\sigma i}) \cdots a_{n\sigma n}$$

$$= \alpha \left(r \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{1\sigma 1} \cdots a_{i\sigma i} \cdots a_{n\sigma n} \right)$$

$$= \alpha f(X_1, \ldots, X_i, \ldots, X_n).$$

We now show that f is additive, i.e., for each i

$$f(X_1, \ldots, X_i + Y_i, \ldots, X_n) = f(X_1, \ldots, X_i, \ldots, X_n) + f(X_1, \ldots, Y_i, \ldots, X_n)$$

where $X_i = (a_{i1}, \ldots, a_{ij}, \ldots, a_{in})$ and $Y_i = (b_{i1}, \ldots, b_{ij}, \ldots, b_{in})$.

Fix a σ and consider the corresponding summand

$$r(\operatorname{sgn}\sigma)\, a_{1\sigma 1} \cdots a_{i\sigma i} \cdots a_{n\sigma n} \quad \text{of} \quad f(X_1, \ldots, X_i, \ldots, X_n);$$

this summand for $f(X_1, \ldots, X_i + Y_i, \ldots, X_n)$ becomes

$$r(\operatorname{sgn}\sigma)\, a_{1\sigma 1} \cdots (a_{i\sigma i} + b_{i\sigma i}) \cdots a_{n\sigma n}$$

$$= r(\operatorname{sgn}\sigma)\, a_{1\sigma 1} \cdots a_{i\sigma i} \cdots a_{n\sigma n} + r(\operatorname{sgn}\sigma)\, a_{1\sigma 1} \cdots b_{i\sigma i} \cdots a_{n\sigma n}.$$

Now sum up for each σ. Hence f is multilinear.

We show now that $f(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = r$.

Note $\varepsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where 1 appears at the ith place, whence for a typical summand

$$r(\operatorname{sgn}\sigma)\, a_{1\sigma 1} \cdots a_{n\sigma n} = 0 \quad \text{if even for one } i \ \ \sigma(i) \neq i.$$

If $\sigma \neq \mathrm{id}$, then the corresponding summand $= 0$ in the whole sum, only the term corresponding to id remains, i.e.,

$$f(\varepsilon_1, \ldots, \varepsilon_n) = r(\operatorname{sgn}\sigma)\, a_{11} a_{22} \cdots a_{nn}.$$

$$= r(1)(1)(1) \cdots (1) = r$$

Finally we prove that f is alternating,

i.e., $f(X_1, \ldots, X_n) = 0$ if $X_i = X_j$ for $i \neq j$.

Without loss of generality, suppose $\rho = (1\ 2)$ and the map $\phi : A_n \to S_n$ given $\phi(\sigma) = \sigma\rho$.

We claim that ϕ is injective. ($\phi(A_n)$ is the set of all odd

permutations.) For if

$$\phi(\sigma_1) = \phi(\sigma_2), \quad \text{then} \quad \phi(\phi(\sigma_1)) = \phi(\phi(\sigma_2))$$

$$\Rightarrow \sigma_1 \rho^2 = \sigma_2 \rho^2 \Rightarrow \sigma_1 = \sigma_2, \text{ as } \rho^2 = id.$$

Since σ is even, $\sigma\rho$ is odd:

Since by injectivity and by the fact $|A_n| = \frac{n!}{2}$.

$$|\phi(A_n)| = \frac{n!}{2}$$

and the number of odd permutations $= \frac{n!}{2}$

Hence $S_n = A_n \bigcup \{A_n\rho\}$.

Now consider

$$f(X_1, X_1, X_3, \ldots, X_n) = r \sum_{\sigma \in S_n} (\text{sgn } \sigma)(a_{1\sigma 1})(a_{2\sigma 2}) \ldots (a_{n\sigma n}).$$

In this sum, let us consider the summand (or the term) corresponding to an even permutation σ.

$$r(\text{sgn } \sigma)\, a_{1\sigma 1}\, a_{2\sigma 2} \ldots a_{n\sigma n} = r(\text{sgn } \sigma)\, a_{2\sigma 1} a_{1\sigma 2} \ldots a_{n\sigma n}$$

Since $X_1 = X_2$,

$$a_{1\sigma 1} = a_{2\sigma 1},$$

$$a_{2\sigma 2} = a_{1\sigma 2}. \quad \text{(indeed } a_{1j} = a_{2j} \text{ for all } j).$$

Now consider the term corresponding to the odd permutation $\sigma\rho$. $\sigma\rho$ is different from σ only at 1 and 2.

Now $\text{sgn } \sigma = +1$. $\text{sgn } \sigma\rho = -1$. Hence the term corresponding to $\sigma\rho$ is $r(-1)\, a_{1\sigma\rho(1)}\, a_{2\sigma\rho(2)} \ldots a_{n\sigma\rho(n)} = -r a_{1\sigma(1)}\, a_{2\sigma(1)} \ldots a_{n\sigma(n)}$.

Hence the term corresponding to $\sigma\rho$ is the negative of the term corresponding to σ, and thus

$$f(X_1, X_1, X_3, \ldots, X_n) = 0.$$

Remark: A multilinear form on $\mathrm{Mat}_n R$ is an R-multilinear form on $(R^n)^n$ whose arguments are the rows of $n \times n$ matrices considered as elements of R^n.

2.4.6 Definition: Let R be a commutative ring with identity. The unique alternating R-multilinear form $d : \mathrm{Mat}_n R \to R$ such that $d(I_n) = 1_R$ is called the determinant function on $\mathrm{Mat}_n R$. (The determinant of a matrix $A \in \mathrm{Mat}_n R$ is the element $d(A) \in R$ and is denoted $|A|$.)

2.4.7 Theorem: Let $A, B \in \mathrm{Mat}_n R$. Then

(i) Every alternating R-multilinear form f on $\mathrm{Mat}_n R$ is a unique scalar multiple of the determinant function d.

(ii) If $A = (a_{ij})$, then $|A| = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{1\sigma 1}\, a_{2\sigma 2} \cdots a_{n\sigma n}$.

(iii) $|AB| = |A|\ |B|$.

(iv) If A is invertible in $\mathrm{Mat}_n R$, then $|A|$ is a unit in R.

Proof: (i) Let $f(I_n) = r \in R$. Let d be the determinant function. The function $rd : \mathrm{Mat}_n R \to R$ given by $A \longmapsto r|A| = rd(A)$ is R-multilinear form on $\mathrm{Mat}_n R$;

$(rd)(b_1, b_2, \ldots, b_n) = rd(b_1, \ldots, b_n)$ where b_i is the ith row of Matrix A.

$$(rd)(b_1,b_2,\ldots,b_{i-1},sb+tb',b_{i+1},\ldots,b_n) = rd(b_1,\ldots,b_{i-1},$$
$$sb+tb',b_{i+1},\ldots,b_n)$$
$$= r\{sd(b_1,\ldots,b,\ldots,b_n) + td(b_1,\ldots,b',\ldots,b_n)\}$$
$$= srd(b_1,\ldots,b,\ldots,b_n) + trd(b_1,\ldots,b',\ldots,b_n)$$
$$= s(rd)(b_1,\ldots,b,\ldots,b_n) + t(rd)(b_1,\ldots,b',\ldots,b_n)$$

$rd(A)$ is also an alternating function, for $(rd)(b_1,b_1,\ldots,b_n)$ $= rd(b_1,b_1,\ldots,b_n) = r.0 = 0$ whenever $b_i = b_j$ for some $i \neq j$. Hence $rd(A)$ is an alternating R-multilinear form on Mat_nR such that $rd(I_n) = r$, whence $f = rd$ by the uniqueness statement of theorem 2.4.5. Suppose $f = rd = sd$. Then $f(I_n) = rd(I_n) = sd(I_n) = sd(I_n) \Rightarrow r = s$, whence the uniqueness of r.

(ii) It is nothing more than a restatement of the equation

$$f(X_1,\ldots,X_n) = r \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\, a_{1\sigma 1}a_{2\sigma 2}\cdots a_{n\sigma n}$$

by replacing r by 1.

(iii) Let B be fixed and denote the columns of B by $Y_1,Y_2,\ldots,Y_n$. If C is any $n \times n$ matrix with rows $X_1,\ldots,X_n$, then the (i,j) entry of CB is $(X_iY_1, X_iY_2,\ldots, X_iY_n)$. Now suppose $CB = (A_{ij})$. Consider

$$f:(R^n)^n \cong Mat_n(R) \to R$$

given by $C \mapsto |CB|$.

Using formula (ii) in theorem 2.4.7. $|CB| = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) A_{1\sigma 1} \cdots A_{1\sigma(n)}$

$$= \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, X_i\, Y_{\sigma(1)} \cdots X_i\, Y_{\sigma(i)} \cdots X_n\, Y_{\sigma(n)}.$$

Suppose we consider ith row of C, and instead of X_i, we have say $X_i^1 + X_i^2$ (say C^1 corresponds to X_i^1) then

$$f(\ldots, X_i^1 + X_i, \ldots) = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) X_1 Y_{\sigma(1)} \cdots (X_i^1 + X_i^2) Y_{\sigma(i)} \cdots X_n Y_{\sigma(n)}$$

$$= \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) X_1 Y_{\sigma(1)} \cdots X_i^1 Y_{\sigma(i)} \cdots X_n Y_{\sigma(n)} +$$

$$\sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) X_1 Y_{\sigma(1)} \cdots X_i^2 Y_{\sigma(i)} \cdots X_n Y_{\sigma(n)} .$$

$$= f(X_1, \ldots, X_i^1, \ldots, X_n) + f(X_1, \ldots, X_i^2, \ldots,$$

$$f(X_1, \ldots, X_i^2, \ldots, X_n)$$

Similar argument holds for scalar multiplication.

We want to show $f(X_1, \ldots, X_n) = 0$ if $X_i = X_j$.

Assume for convenience $i = 1$, $j = 2$. Let $\rho = (1, 2)$.

If $\sigma \in S_n$ is even, then summand of $f(X_1, X_1, \ldots, X_n)$ corresponding to σ is $+ a_{1\sigma 1}\, a_{2\sigma 2} \cdots a_{n\sigma n}$. Therefore $a_{1\sigma(1)} = a_{2\sigma(1)}$ and $a_{2\sigma(2)} = a_{1\sigma(2)}$. Also the summand corresponding to the odd permutation $\sigma\rho$ is $- a_{1\sigma\rho(1)}\, a_{2\sigma\rho(2)} \cdots$

$a_{n\sigma\rho(n)} = - a_{1\sigma(2)}\, a_{2\sigma(1)} \cdots a_{n\sigma(n)} = - a_{2\sigma(2)}\, a_{1\sigma(1)} \cdots$

$a_{n\sigma(n)} = - a_{1\sigma(1)}\, a_{2\sigma(2)} \cdots a_{n\sigma(n)}$. Hence the result.

Therefore we conclude that f is an alternating R-multilinear form f on $\mathrm{Mat}_n R$. By (i) above $f = rd$ for some $r \in R$. Consequently,

$$|CB| = f(C) = rd(C) = r\,|C| .$$

In particular,

$$|B| = |I_n\, B| = r|I_n| = r,$$

whence

$$|AB| = r\,|A| = |A|\,|B| .$$

(iv) $AA^{-1} = I_n$ implies $|A|\,|A^{-1}| = |AA^{-1}| = |I_n| = 1$ by (iii). Hence $|A|$ is a unit in R with $|A|^{-1} = |A^{-1}|$.

2.4.8 Theorem: Let $A, B \in \mathrm{Mat}_n R$, then:

(i) If A and B are similar, then $|A| = |B|$.

(ii) $|A^t| = |A|$.

(iii) If $A = (a_{ij})$ is triangular, then $|A| = a_{11}\, a_{22} \cdots a_{nn}$.

(iv) If B is obtained by interchanging two rows (columns) of A, then $|B| = -|A|$.

If B is obtained by multiplying one row (column) of A by $r \in R$, then $|B| = r\,|A|$.

If B is obtained by adding a scalar multiple of row i

(column i) to row j (column j) ($i \neq j$), then $|B| = |A|$.

Proof: (i) $B = PAP^{-1} \Rightarrow |B| = |P|\,|A|\,|P^{-1}| = |A|$ since R is commutative.

(ii) Let $A = (a_{ij})$. If $i_1, \ldots, i_n$ are integers $1, 2, \ldots, n$ in some order, then since R is commutative any product $a_{i1}\, a_{i2}\, a_{i3} \cdots a_{in}$ may be written as $a_{ij_1}\, a_{2j_2} \cdots a_{njn}$. For if σ is the permutation such that $\sigma(k) = i_k$, then σ^{-1} is the permutation such that $\sigma^{-1}(i_k) = k$. Furthermore, for any $\sigma \in S_n$, $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$. Let $A^t = (b_{ij})$; then since S_n is a group,

$$|A^t| = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, b_{1\sigma 1} \cdots b_{n\sigma n}$$

$$= \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{\sigma 1 1} \cdots a_{\sigma n n}$$

$$= \sum_{\sigma^{-1} \in S_n} (\operatorname{sgn} \sigma^{-1})\, a_{1\sigma_1^{-1}} \cdots a_{n\sigma_n^{-1}}$$

$$= |A|.$$

(iii) By hypothesis either $a_{ij} = 0$ for all $j < i$ or $a_{ij} = 0$ for all $j > i$, if $\sigma \in S_n$ and $\sigma \neq (1)$, then

$$a_{1\sigma 1} \cdots a_{n\sigma n} = 0$$

(there is at least one i such that $\sigma(i) < i$ or $\sigma(i) > i$)

whence

$$|A| = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma)\, a_{1\sigma 1} \cdots a_{n\sigma n}$$

$$= a_{11}\, a_{22} \cdots a_{nn}\,.$$

(iv) Let $X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n$ be the rows of A. If B has rows $X_1, \ldots, X_j, \ldots, X_i, \ldots, X_n$, then since d is skew-symmetric by theorem 1.4.4

$$|B| = d(X_1, \ldots, X_j, \ldots, X_i, \ldots, X_n)$$

$$= -d(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n)$$

$$= -|A|\,.$$

Similarly if B has rows $X_1, \ldots, X_i, \ldots, rX_i + X_j, \ldots, X_n$ then since d is multilinear and alternating

$$|B| = d(X_1, \ldots, X_i, \ldots, rX_i + X_j, \ldots, X_n)$$

$$= rd(X_1, \ldots, X_i, \ldots, X_i, \ldots, X_n) + d(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n)$$

$$= r.0 + |A$$

$$= |A|$$

The other statement is proved similarly; we use (i) for the corresponding statements about columns.

Remark: More generally, the determinant of an $n \times n$ matrix A over any commutative ring with identity may be calculated according the following proposition.

For each pair (i, j) let A_{ij} be the $(n-1) \times (n-1)$ matrix obtained by deleting row i and column j from A. Then $|A_{ij}| \in R$ is called the <u>minor</u> of $A = (a_{ij})$ at position (i, j) and $(-1)^{i+j} |A_{ij}| \in R$ is called the <u>cofactor</u> of a_{ij}.

2.4.9 <u>Proposition</u>: If A is an $n \times n$ matrix over a commutative ring R with identity; then for each $i = 1, 2, \ldots, n$,

$$|A| = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}| ,$$

and for each $j = 1, 2, \ldots, n$,

$$|A| = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}| .$$

<u>Proof</u>: We let j be fixed and prove the second statement. By theorem 2.4.5 and Definition 2.4.6 it is sufficient to show that map $\phi : \mathrm{Mat}_n R \to R$ given by

$$A = (a_{ij}) \longmapsto \sum_{i=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}|$$

is an alternating R-multilinear form such that $\phi(I_n) = 1$. To show that ϕ is alternating, let $X_1, \ldots, X_n$ be the rows of A. If $X_k = X_t$ with $1 \leq k < t \leq n$, then $|A_{ij}| = 0$ for $i \neq k, t$ since it is the determinant of a matrix with two identical rows. Since A_{kj} may be obtained from A_t; by interchanging row t successively with rows $t-1, \ldots, k+1$, $|A_{kj}| = (-1)^{t-k-1} |A_{tj}|$ by theorem 2.4.8 (iv). Thus

$$\phi(A) = (-1)^{k+j} |A_{kj}| + (-1)^{t+j} |A_{tj}|$$

$$= (-1)^{k+j+t-k-1} |A_{tj}| + (-1)^{t+j} |A_{tj}|$$

$$= 0 .$$

Hence ϕ is alternating.

Now we show that ϕ is R-multilinear. Let

$$X_k + rX_k + sW_k \quad \text{for some } k.$$

Let $B = (b_{ij})$ and $C = (c_{ij})$ be the matrices with rows $X_1, \ldots, X_{n-1}, Y_k, X_{k+1}, \ldots, X_n$ and $X_1, \ldots, X_{k-1}, W_k, X_{k+1}, \ldots, X_n$ respectively. To prove that ϕ is R-multilinear we need only show that $\phi(A) = r\phi(B) + s\,\phi(C)$.

If $i = k$, then $|A_{kj}| = |B_{kj}| = |C_{kj}|$, whence

$$a_{kj} |A_{kj}| = (rb_{kj} + sc_{kj}) |A_{kj}|$$

$$= rb_{kj} |B_{kj}| + sc_{kj} |C_{kj}|.$$

If $i \neq j$, then since each $|A_{ij}|$ is a multilinear function of the rows of A_{ij} and $a_{ij} = b_{ij} = c_{ij}$ for $i \neq k$, we have

$$a_{ij} |A_{ij}| = a_{ij} (r |B_{ij}| + s |C_{ij}|)$$

$$= rb_{ij} |B_{ij}| + sc_{ij} |C_{ij}| .$$

It follows that

$$\phi(A) = r\phi(B) + s\phi(C), \text{ hence } \phi \text{ is R-multilinear.}$$

Obviously

$$\phi(I_n) = 1.$$

Therefore, ϕ is the determinant function.

The first statement of thetheorem follows readily through the use of transposes.

Remark: (i) Thefirst formula for $|A|$ in proposition 2.4.9 is called the expansion of $|A|$ along row i.

(ii) The second formula for $|A|$ in proposition 2.4.9 is called the expansion of $|A|$ along column j.

2.4.10 Proposition: If $A = (a_{ij})$ is an $n \times n$ matrix over a commutative ring R with identity and $A^a = (b_{ij})$ is the $n \times n$ matrix with

$$b_{ij} = (-1)^{i+j} |A_{ji}| ,$$

then

$$AA^a = |A| I_n = A^a A.$$

Furthermore,

A is invertible in $Mat_n R$ if and only if $|A|$ is a unit in R, in which case

$$A^{-1} = |A|^{-1} A^a .$$

Proof: The (i, j) entry of AA^a is

$$C_{ij} = \sum_{k=1}^{n} (-1)^{j+k} a_{ik} |A_{jk}| .$$

If $i = j$, then $c_{ii} = |A|$ by Proposition 2.4.9. Let $i \neq j$ (say $i < j$) and A have rows $X_1, \ldots, X_n$ and let $B = (b_{ij})$ be the matrix with rows

$$X_1, \ldots, X_i, \ldots, X_{j-1}, X_i, X_{j+1}, \ldots, X_n .$$

Then

$$b_{ik} = a_{ik} = b_{jk}$$

and

$$|A_{jk}| = |B_{jk}| \quad \text{for all } k ;$$

in particular, $|B| = 0$ since the determinant is an alternating form. Hence

$$C_{ij} = \sum_{k=1}^{n} (-1)^{j+k} a_{ik} |A_{jk}|$$

$$= \sum_{k=1}^{n} (-1)^{j+k} b_{jk} |B_{jk}|$$

$$= |B|$$

$$= 0.$$

Therefore, $C_{ij} = \delta_{ij} |A|$ (Kronecker delta) and $AA^a = |A| I_n$.

In particular, the last statement holds with A^t in place of A

$$A^t (A^t)^a = |A^t| \, I_n .$$

Since $(A^a)^t = (A^t)^a$, we have $|A| \, I_n = |A^t| \, I_n$

$$= A^t (A^t)^a = A^t (A^a)^t = (A^a A)^t ,$$

whence

$$A^a A = (\, |A| \, I_n)^t = A \, |I_n| .$$

Thus if $|A|$ is a unit in R, $|A|^{-1} A^a \in \mathrm{Mat}_n R$ and clearly $(|A|^{-1} A^a) A = I_n = A(|A|^{-1} A^a)$.

Hence A is invertible with (necessarily unique) inverse $A^{-1} = |A|^{-1} A^a$.

Conversely, if A is invertible, then $|A|$ is a unit by theorem 2.4.7 (iv).

Remark: The matrix A^a is called the classical adjoint of A.

Note that if R is a field, then $|A|$ is a unit iff $|A| \neq 0$.

CHAPTER III

ELEMENTARY DIVISORS

3.1 Introduction and basic definitions

R will denote a commutative ring with identity unless otherwise specified.

We shall have occasion to consider matrices over the ring R. We shall denote the ring of matrices of type $m \times n$ by R_{mxn}.

A square matrix A of type $n \times n$ is called non-singular if there exists a matrix B such that $AB = I$, where I is the identity matrix. As already shown earlier, a matrix is non-singular if and only if its determinant is an invertible element in the ring R.

We are interested in studying the possibility of reducing a given matrix over R to a simpler form.

For typographical reasons we shall write

$$\text{diag}\ (d_1, d_2, \ldots\ )$$

for a matrix of type $m \times n$ having $d_1, d_2, \ldots$ down the main diagonal (i.e., starting upper left-hand corner) and zero everywhere else.

Matrices will be denoted by capital latin letters except R where R is reserved to denote a ring.

3.1.1 Definition: An $m \times n$ matrix A over R "admits triangular reduction" if there exist non-singular matrices U, V such that

$$AU = (b_{ij})$$

is upper triangular (i.e., $b_{ij} = 0$ whenever $i > j$), and VA is lower triangular.

3.1.2 Definition: The matrix A "admits diagonal reduction" if there exist non-singular matrices P, Q such that

$$PAQ = \text{diag}\,(d_1, d_2, \ldots) \qquad \ldots \quad (1)$$

and d_i is a divisor of d_{i+1}.

3.1.3 Definition: A ring R over which every matrix admits diagonal reduction is called an elementary divisor ring.

Suppose A is $1 \times n$ (or $m \times 1$) matrix then either P or Q in (1) is a 1×1 invertible matrix, hence can be deleted. In this case triangular reduction is equivalent to diagonal reduction.

As will be proved later if all 1×2, 2×1 and 2×2 matrices admit diagonal reduction, then every matrix admits triangular reduction. Hence, we make the following definition.

3.1.4 Definition: A ring R is called a Hermite ring, if every 1×2 matrix over R admits diagonal reduction.

In other words, if A is 1×2 matrix $(a \quad b)$ over a Hermite ring, then there exists a 2×2 non-singular matrix Q such that

$$(a \quad b)\, Q = (d \quad 0) \qquad \ldots \quad (2)$$

Remarks: 1. The notion of a Hermite ring and that of an elementary divisor ring are due to Kaplansky who first studied them in [K].

2. Note that if every 1×2 matrix admits diagonal reduction then every 2×1 admits diagonal reduction by using transposes, as shown below:

Suppose 1×2 admits diagonal reduction, then 2×1 also admits diagonal reduction.

Let A be 2×1 matrix $\begin{pmatrix} a \\ b \end{pmatrix}$, then consider the transpose matrix which is

$$A^T = (a \quad b)$$

A^T admits a diagonal reduction, therefore there exists a 2×2 non-singular matrix Q such that

$$(a \quad b)\, Q = (d \quad 0)$$

Therefore;

$$Q^T \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

and Q^T is non-singular.

3.2 Hermite Rings

In this section we shall study Hermite rings and give some of their properties.

3.2.1 Proposition: Every Hermite ring is an F-ring.

Proof: We want to show that the sum of two principal ideals is a principal ideal.

Let (a) and (b) be two principal ideals. We want to show that;

$(a, b) = (a) + (b) = (c)$ for some c in R.

Consider the 1×2 matrix $(a \quad b)$ then there exists a 2×2 non-singular matrix $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ such that

$$(a \quad b) \begin{pmatrix} x & y \\ z & w \end{pmatrix} = (c \quad 0)$$

Hence $ax + bz = c$. ---- (1)

Using the fact that A is invertible,

$$(a \quad b) = (c \quad 0) \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}$$

Therefore,

$$a = cx' \quad \text{and} \quad b = cy' \qquad \text{---} \quad (2)$$

Take an element of $(a) + (b)$, say $ra + sb$ such that $r, s \in R$. We want to show that $ra + sb = tc$ for some $t \in R$. We have

$$ra + sb = r(cx') + s(cy') = rcx' + scy' = c(rx' + sy').$$

Take $rx' + sy'$ to be our t, therefore

$$(a) + (b) \quad (c)$$

Now we want to show that

$$c \in (a) + (b).$$

Since $c = ax + bz$

$$(c) \subseteq (a) + (b) \quad \text{and hence} \quad (c) = (a, b).$$

In general there are F-rings which are not Hermite rings (Example given later). However, the following discussion indicates the difficulties involved. Suppose R is an F-ring, does every $(a \quad b)$ admit a diagonal reduction to $(d \quad 0)$.

First let us consider the following matrices in R_2:

$$A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad D = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix}$$

We claim that if $aR + bR = dR$, then the above two matrices are right multiples of each other. Indeed there exist $x, y, \alpha, \beta \in R$ such that

$ax + by = d$,

$a = d\alpha$,

$b = d\beta$.

Let Q be the matrix $\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$ and $Q' = \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}$.

Then it is easy to see that $AQ = D$ and $DQ' = A$. What we want is to choose Q or Q' to be invertible. In other words we want to know, if two elements in R_2 are right multiples of one another, then whether they are right associates. However, this is not true even if the ring is commutative.

3.2.2 Example: Let R be the ring of continuous functions on $]0, 3[$. Let

$$a(t) = \begin{cases} 1 - t & \text{for }]0, 1[\\ 0 & \text{for }]1, 2[\\ t - 2 & \text{for }]2, 3[\end{cases}$$

and

$$b(t) = \begin{cases} 1 - t & \text{for }]0, 1[\\ 0 & \text{for }]1, 2[\\ 2 - t & \text{for }]2, 3[\end{cases}$$

Then $a(t)$ and $b(t)$ are multiples of each other but they are not associates.

3.2.3 Lemma: Let R be a ring in which all right divisors of zero are in the radical of R. If $aR = bR$, then a and b are right associates.

Proof: $a = by$ and $b = ax$, then $a = axy$. If $a, b = 0$ there is nothing to prove, otherwise,

$$a - axy = 0 \Rightarrow a(1 - xy) = 0$$

Hence $1 - xy \in$ radical $\Rightarrow 1 - (1 - xy)$ is a unit in R (by 1.4.9). Hence xy is a unit in R, so x and y are units in R. Therefore a and b are associates.

Open Question: Let R be a ring in which all right zero divisors are in the radical. Is it true for R_2?

However, let us now state and prove Kaplansky's main theorem.

3.2.4 Theorem: Let R be a ring in which finitely generated ideals are principal and zero divisors of R are contained in the radical of R. Then it is a Hermite ring.

Proof: Take $A = (a \quad b)$ be a 1×2 matrix. We want to find a non-singular $Q = \begin{pmatrix} x & z \\ y & w \end{pmatrix}$ so that

$$AQ = (d \quad Q).$$

Consider the ideal $aR + bR$. By the hypothesis

$$aR + bR = dR \text{ for some } d.$$

Then

$$d = ax + by \quad \text{for some} \quad x, y \in R \quad \text{and},$$

$$a = dw, \quad b = -dz \quad \text{for some} \quad w, z \quad \text{in} \quad R.$$

Then

$$dxw - dyz - d = 0,$$

$$d(xw - yz - 1) = 0.$$

If $d = 0$, then $a, b = 0$. There is nothing to prove. If $d \neq 0$, then $xw - yz - 1$ is a zero divisor, whence

$$xw - yz - 1 \in \text{rad } R.$$

Hence, by (1.4.9), $yz - xw$ is a unit in R.

Thus the matrix

$$Q = \begin{pmatrix} x & z \\ y & w \end{pmatrix} \quad \text{is invertible,}$$

and $AQ = (d \quad 0)$.

3.2.5 Corollary: An integral domain is a Hermite ring if and only if it is a Bezout domain.

Proof: $\Rightarrow$ by 3.2.1

$\Leftarrow$ since R is an integral domain, the set of zero divisor = $\{0\}$ and $\{0\} \subseteq$ rad R. Since in a Bezout ring finitely generated ideals are principal, the corollary follows from (3.2.4).

Remark: Kaplansky ([K], Theorem 3.1 and Theorem 3.4, pages 467 and 468) gives a set of rather lengthy sufficient conditions (which are also necessary in case of rings without divisors of zero) for a general ring (not necessarily commutative) to be Hermite.

We shall state the theorem without proving it.

Theorem [K]: Let R be a ring satisfying the following conditions:

(i) All divisors of zero are in the radical.

(ii) The union and intersection of any two principal right ideals is a principal right ideal.

(iii) The union of any two principal left ideals is a principal left ideal.

(iv) In R_2 a matrix with one sided inverse is non-singular.

Then R is a right Hermite ring. And conversely, if R has no divisors of zero then a necessary and sufficient condition for R to be a Hermite ring is that the union and intersection of any two principal right or left ideals be principal.

For proof see [K], pages 467 and 468.

Returning back to the commutative case we prove the following theorem due to Gillman and Henriksen, characterizing a commutative Hermite ring.

3.2.6 Theorem (Gillman and Henriksen): Let R be a commutative ring with identity, then R is a Hermite ring if and only if it satisfies

the condition (T): for all $a, b \in R$ there exist $u, v, s, t, d \in R$ such that,

$$a = ud \quad , \quad b = vd \quad \text{and}$$

$$su + tv = 1$$

Proof: Suppose R satisfies condition (T). Let $a, b \in R$, we want to find a diagonal reduction for the matrix $A = (a \quad b)$. By (T) there exist $u, v, s, t, d \in R$ such that

$$a = ud \quad , \quad b = vd \quad \text{and}$$

$$su + tv = 1$$

Let $Q = \begin{pmatrix} s & -v \\ t & u \end{pmatrix}$.

Clearly Q is non-singular.

Now $AQ = (a \quad b) \begin{pmatrix} s & -v \\ t & u \end{pmatrix}$

$$= (as + bt \quad - \quad av + bu)$$

$$= (d \qquad 0)$$

Conversely, let R be a Hermite ring. Let $a, b \in R$. By hypothesis there exists a non-singular matrix

$$P = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \quad \text{such that}$$

$$AP = (c \quad 0),$$

$$(a \quad b) \begin{pmatrix} p & r \\ q & s \end{pmatrix} = (ap + bq \quad ar + bs) = (c \quad 0)$$

Hence (1) $ap + bq = c$

(2) $ar + bs = 0$

(3) $ps - rq = 1$ [This is a unit, so without loss of generality, we can take it to be 1].

Thus $aps - arq = a \Rightarrow aps + qsb = a$

$\Rightarrow s(ap + qb) = a \Rightarrow sc = a.$

Similarly, $b = -rc.$

Finally, $sp + q(-r) = 1.$

3.3 Triangular Reduction

In this section we prove a result due to Kaplansky [K], which shows that triangular reduction of matrices is possible over a Hermite ring.

3.3.1 Theorem: For any matrix A over a Hermite ring R, we can find a non-singular matrix U such that AU is lower triangular (i.e., A admits a triangular reduction.)

Proof: Let A be an $m \times n$ matrix. First we treat the case $m = 1$ (A is a single row).

If n is also equal to 1, nothing to prove. So assume $n > 1$. The case $n = 2$ follows from the definition of a Hermite ring. Hence we suppose $n > 2$ and write $A = (a, B)$ where B is a $1 \times n-1$ matrix. We suppose the result to be true for all integers

strictly less than n. Hence there exists a non-singular $(n-1) \times (n-1)$ matrix V such that

$$BV = (b \quad 0 \ldots 0).$$

Now, since R is a Hermite ring, there exist a non-singular 2 by 2 matrix W such that,

$$(a \quad b)\, W = (d \quad 0).$$

Set

$$U = \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix} \begin{pmatrix} W & 0 \\ 0 & I \end{pmatrix}$$

Then U is an $n \times n$ non-singular matrix.

Now

$$AU = (a \quad B) \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix} \begin{pmatrix} W & 0 \\ 0 & I \end{pmatrix}$$

$$= (a \quad BV) \begin{pmatrix} W & 0 \\ 0 & I \end{pmatrix}$$

$$= (a \quad b \quad 0 \ldots 0) \begin{pmatrix} W & 0 \\ 0 & I \end{pmatrix}$$

$$= (d \quad 0 \quad 0 \ldots 0)$$

This concludes the proof for $m = 1$ and n arbitrary. Suppose the theorem is true for any integer strictly less than m and n, where m and n are arbitrary, but fixed integers.

Now, let A be any rectangular matrix. By induction (considering only the first row of A), there exists a non-singular matrix V of order n such that

$$AV = \begin{pmatrix} a & 0 \\ B & C \end{pmatrix},$$

where C is an $(m-1) \times (n-1)$ matrix.

By induction hypothesis there exists a non-singular matrix W such that CW is lower triangular (that is, has zeros above the main diagonal). Then, let

$$U = V \begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix},$$

so U is an $n \times n$ non-singular matrix.

Also
$$AU = AV \begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 \\ B & C \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 \\ B & CW \end{pmatrix}$$

is a lower triangular matrix.

Remark: By symmetry we can find a matrix V such that VA is an upper triangular.

As a bonus we have the following theorem.

3.3.2 Theorem: If R is a Hermite ring, so is R_n.

Proof: By symmetry it is enough to show it for right Hermite rings. Let $A, B \in R_n$, then $(A \quad B)$ is an $n \times 2n$ matrix over R. Hence by previous theorem there exists a $2n \times 2n$ non-singular matrix U such that

$$(A \quad B)\, U$$

is an $n \times 2n$ lower triangular matrix, and hence has the form $(D \quad 0)$, where D is an $n \times n$ matrix.

Remark: Kaplansky proves theorem 3.3.1 for right Hermite rings.

In case the ring R is commutative, then the $1 \times n$ case of Theorem 3.3.1 can be strengthened as follows:

3.3.3 Theorem [K]: Let $a_1, \ldots, a_n$ be elements in a commutative Hermite ring R. Then we can find an $n \times n$ matrix with first row $(a_1 \ldots a_n)$ and determinant d satisfying

$$dR = a_1 R + \ldots + a_n R .$$

Proof: We will use induction and we prove a little bit more, namely, that we can choose the additional $n-1$ rows in such a fashion that they can be completed to a non-singular matrix by induction of a suitable nth row. Hence, by induction, let B be an $(n-2) \times (n-1)$ matrix which when adjointed to $(a_1 \ldots a_n)$ yields determinant e with

$$eR = a_1 R + \ldots + a_{n-1} R ;$$

and let C denote the extra row which makes B non-singular. Since R is a Hermite ring, we can reduce $(e, \ a_n)$, so

$$(e, \ a_n) \begin{pmatrix} p & r \\ q & s \end{pmatrix} = (d \quad 0) \ldots \qquad \ldots \ (1),$$

where $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$ is a non-singular matrix.

Then we have

$$\begin{vmatrix} a_1 & \cdots & a_{n-1} & a_n \\ & B & & 0 \\ (-1)^{n-1}qC & & & p \end{vmatrix} = d$$

For expanding by the last column, we have

$$(-1)^{n-1}a_n \begin{vmatrix} & B & \\ (-1)^{n-1}qc & & \end{vmatrix} + (-1)^{2(n-1)}p \begin{vmatrix} a_1 \cdots a_{n-1} \\ B \end{vmatrix} = a_n q + pe = d \quad \ldots \text{ by (1).}$$

Thus we have found the desired matrix with determinant d.

From (1)

$$eR + a_n R = dR,$$

and by induction

$$eR = a_1 R + \ldots + a_{n-1} R .$$

Therefore we have

$$dR = a_1 R + \ldots + a_{n-1} R + a_n R .$$

To complete the induction we have to show the $(n-1) \times n$ matrix

$\begin{pmatrix} B & 0 \\ (-1)^{n-1}qC & p \end{pmatrix}$ can be completed to a non-singular matrix by

adjoining a suitable row.

Consider the matrix $\begin{pmatrix} B & 0 \\ (-1)^{n-1}qC & p \\ (-1)^{n-1}sC & r \end{pmatrix}$ --- (*)

The determinant of this matrix is equal to

$$r\begin{vmatrix} B \\ (-1)^{n-1}qC \end{vmatrix} - p\begin{vmatrix} B \\ (-1)^{n-1}sC \end{vmatrix}$$

$$= (-1)^{n-1}rq - (-1)^{n-1}ps$$

$$= (-1)^{n}\,[\,ps - rq\,]$$

$$= (-1)^{n}\begin{vmatrix} p & r \\ q & s \end{vmatrix}$$

hence (*) is a non-singular matrix.

3.4 Matrices over F-rings

Let us recall the definition of an F-ring. An F-ring is a ring in which any finitely generated ideal is principal. We know that every Hermite ring is an F-ring (Proposition 3.2.1). Also an F-domain, which is just a Bezout domain is a Hermite ring (Corollary 3.2.5).

Hence it would be interesting to study how far it is possible to obtain triangular reduction of matrices over an F-ring.

It so happens that this can be done by enlarging the matrix with additional columns of zeros. This is the main result of this

section which is due to Kaplansky.

Before stating and proving this result, we need a couple of preparatory lemmas which are also due to Kaplansky. We discuss only the commutative case, which is of interest to us.

3.4.1 Lemma [K]: Let $a, b \in R$ such that they are right multiples of each other (i.e., $aR = bR$). Then there exists a non-singular matrix Q such that

$$(a \quad 0)\, Q = (b \quad 0)$$

Proof: Let $a = by$ and $b = ax$. Consider

$$Q = \begin{pmatrix} x & 1-xy \\ 1 & -y \end{pmatrix}.$$

Then $$(a \quad 0) \begin{pmatrix} x & 1-xy \\ 1 & -y \end{pmatrix} = (ax \quad a-axy)$$

$$= (b \quad 0)$$

We claim

$$Q^{-1} = \begin{pmatrix} y & 1-yx \\ 1 & -x \end{pmatrix}$$

This lemma generalizes as follows:

3.4.2 Lemma [K]: Let R be a commutative ring. Let $a_1, a_2, \ldots, a_n, d \in R$ so that

$$a_1R + a_2R + \ldots + a_nR = dR.$$

Then there exists a non-singular $(n+1) \times (n+1)$ matrix Q such that

$$(a_1 \ldots a_n \ 0)\ Q = (d \quad 0 \ldots 0)$$

Proof: By hypothesis $d = \sum a_i x_i$ and each $a_i = dy_i$.

Let $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ be a column matrix, and

$Y = (y_1 \ldots y_n)$ be a row matrix.

Let

$Q = \begin{pmatrix} X & I-XY \\ 1 & -Y \end{pmatrix}$. Therefore

$$(a_1 \ldots a_n \ 0) \begin{pmatrix} X & I-XY \\ 1 & -Y \end{pmatrix} = (a_1 \ldots a_n \ 0) \begin{pmatrix} x_1 & 1-x_1y_1 \ldots & -x_1y_n \\ x_2 & -x_2y_1 \ \ldots & -x_2y_n \\ \vdots & \vdots & \\ x_n & -x_ny_1 \ \ldots & 1-x_ny_n \\ 1 & y_1 \ \ldots & y_n \end{pmatrix}$$

$$= \left(\sum_{i=1}^{n} a_i x_i \ \ a_1 - \left(\sum_{i=1}^{n} a_i x_i \right) y_1 \ \ldots \ a_j - \left(\sum_{i=1}^{n} a_i x_i \right) y_j \ldots 0 \right)$$

$$= (\ d \quad a_1 - a_1 \quad \ldots \quad 0 \quad \ldots \quad 0\ )$$

$$= (\ d \quad 0 \quad \ldots \quad 0\ ).$$

Now the matrix Q is non-singular since its determinant is 1.

Remark: The above lemma shows that at the expense of adjoining a single zero, we can obtain a triangular reduction of a row matrix.

This and the induction principle leads to:

3.4.3 Theorem [K]: Let R be an F-ring and A be an m-rowed matrix over R, and A_1 the matrix obtained by adjoining m-columns of zeros to A. Then we can find a non-singular matrix U such that A_1U is lower triangular (that is, has zeros above the main diagonal).

Proof: We use induction on the number of rows. The previous Lemma covers the case of $m = 1$.

Let us suppose for induction that the theorem is true for any m-rowed matrix. Let

$$A = \begin{pmatrix} a_{11} & a_{12} \cdots & a_{1n} \\ a_{21} & \cdots & \\ \vdots & & \\ a_{m+1} & & a_{(m+1)n} \end{pmatrix}$$

be an $m+1$ rowed matrix. Consider

$$A' = \begin{pmatrix} a_{11} & a_{12} \cdots & a_{1n} & 0 \\ a_{21} & & & \vdots \\ \vdots & & & \\ a_{m+1} & & a_{(m+1)n} & 0 \end{pmatrix}$$

Let X, Y, etc. ... correspond to the first row and have the same meaning as in the previous lemma. Then

$$\begin{pmatrix} X & I-XY \\ 1 & -Y \end{pmatrix}$$

is an $(n+1)\times(n+1)$ non-singular matrix such that

$$A'U = \begin{pmatrix} d & 0 & \dots & 0 \\ & & B & \end{pmatrix},$$

where B is m-rowed matrix. Therefore we can apply the induction hypothesis for B.

Let B' be the matrix of type $m\times n+m$, which is obtained by adjoining m-columns of zeros to B. Let V be matrix such that $B'V$ is lower triangular. Notice then V is a square matrix of type $n+m$. Consider

$$U' = \begin{pmatrix} X & I-XY & 0 \\ 1 & -Y & \\ 0 & I_{mxm} & \end{pmatrix}$$

Then U' is a non-singular matrix of type $n+1+m$.

Let

$$V' = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & V & \end{pmatrix}$$

Then V' are non-singular of type $m+n+1$.

If A is augmented by $m+1$ zero columns to get A' then

$$A^1U'V' = \begin{pmatrix} d & 0 & \dots & 0 & 0 & \dots & 0 \\ & & & B' & & & 0 \end{pmatrix} V'$$

$$= \begin{pmatrix} d & 0 & \dots & 0 \\ & & B'V & \end{pmatrix}$$ which is lower triangular.

3.5 Reduction of Skew-symmetric matrices

In this section we shall prove another result of Kaplansky which shows that the classical theory of reduction of skew-symmetric matrices is valid over a commutative Hermite ring.

First let us recall some definitions.

3.5.1 Definition: A square matrix $A = (a_{ij})$ is called skew-symmetric if

(i) $a_{ij} = -a_{ji}$ and (ii) $a_{ii} = 0$.

Remark: If the characteristic of the ring is different from 2 then (ii) follows from (i).

3.5.2 Definition: Two matrices A and B over a commutative ring R are congruent if there exists a non-singular matrix P over R such that $P^TAP = B$.

Remark: If A and B are congruent and A is skew-symmetric then B is also skew-symmetric, for let

$$P^TAP = B \quad \text{and} \quad A^T = -A.$$

Then $$(P^TAP)^T = B^T = P^TA^TP = P^T(-A)P = -P^TAP = -B$$

3.5.3 Theorem [K]: Let R be a commutative Hermite ring and A be an $n \times n$ skew-symmetric matrix over R. Then A is congruent to

$$\begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ & & \ddots \\ 0 & & \end{pmatrix},$$

where $A_i = \begin{pmatrix} 0 & a_i \\ -a_i & 0 \end{pmatrix}$, and $a_i \mid a_{i+1}$.

In case n is odd we add a 1×1 zero matrix at the end.

Proof: Let

$$A = \begin{pmatrix} 0 & a_{11} & a_{12} & \cdots & a_{1n} \\ -a_{11} & & & & \\ \vdots & & & & \\ -a_{1n} & & \cdots & & 0 \end{pmatrix},$$

where A is $(n+1) \times (n+1)$ matrix. Consider $(a_{11}\ a_{12} \ldots a_{1n})$. By 3.3.1, there exists a non-singular matrix U over R such that

$$(a_{11} \ldots a_{1n})\, U = (d \quad 0 \ldots 0),$$

and so by commutativity

$$U^T \begin{pmatrix} -a_{11} \\ \vdots \\ -a_{1n} \end{pmatrix} = \begin{pmatrix} -d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

If $W = \begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix}$, then

$W^T A W$ is of the form

$$\begin{pmatrix} 0 & b_1 & 0 & \dots & 0 \\ -b_1 & & & & \\ 0 & & & & \\ \vdots & & & G & \\ 0 & & & & \end{pmatrix},$$

where G is skew-symmetric of order $n \times n$. we claim, every skew-symmetric matrix over a commutative Hermite ring is congruent to a matrix B where the diagonal above and below the main diagonal are non-zero and the rest of the entries are zeros.

This is trivially true for any 1×1 skew-symmetric matrix. Suppose it is true for any $n \times n$ matrix, then the above argument shows that the claim is also true for $(n+1) \times (n+1)$ matrix and therefore by induction, the proof of the claim is complete.

Hence to prove the theorem we may assume our matrix A is congruent to a matrix of the form

$$B = \begin{pmatrix} 0 & b_1 & 0 & \dots & 0 \\ -b_1 & 0 & b_2 & \dots & \\ 0 & -b_2 & 0 & b_3 & \dots \\ \vdots & & & & \\ 0 & & \dots & & 0 \end{pmatrix}$$

Let P be an $n \times n$ non-singular matrix such that

$$(b_1 \dots b_n)^t P = (d \quad 0 \dots 0) \quad \text{(by Theorem 3.3.1).}$$

Now to the ith row of P for $(2 \leq i \leq n-1)$ add the sum of all the previous rows. Let the resulting matrix be P'. Let

$$Q = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & & & \\ 1 & & P' & \\ 0 & & & \end{pmatrix}$$

Since P is non-singular, Q is also non-singular.

A direct computation shows

$$Q^T B Q = C,$$

where the first row of C is given by $(0 \quad d \ \ldots)$, and d divides all the other entries of C.

Now we proceed to sweep out the first and second rows and columns to get a matrix

$$\begin{pmatrix} 0 & d & 0 & \cdots & 0 \\ -d & 0 & & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & & \\ 0 & 0 & & B_1 & \end{pmatrix}$$

Now by induction B_1 is congruent to a skew-symmetric matrix which satisfies the condition of the theorem, i.e., there exist an $n \times n$ non-singular matrix N such that

$$N^T B_1 N = \begin{pmatrix} A_2 & & & 0 \\ & A_3 & & \\ & & \ddots & \\ 0 & & & \end{pmatrix},$$

where A_i is of the form $\begin{pmatrix} 0 & a_i \\ -a_i & 0 \end{pmatrix}$ and $a_i \mid a_{i+1}$.

Consider

$$N_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix},$$

then

$$N_1^T C N_1 = \begin{pmatrix} A_1 & & 0 \\ & A_2 & \ddots \\ 0 & & \end{pmatrix},$$

where

$$A_1 = \begin{pmatrix} 0 & d \\ -d & 0 \end{pmatrix} \quad \text{and} \quad d \mid a_2 .$$

Hence the proof of the theorem is complete.

Remark: Consider the matrix

$$A = \begin{pmatrix} 0 & a & b \\ -a & 0 & 0 \\ -b & 0 & 0 \end{pmatrix}$$

over a commutative ring R. If A is congruent to

$$D = \begin{pmatrix} 0 & d & 0 \\ -d & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

then $aR + bR = dR$, i.e., R is an F-ring.

Thus, in order that the reduction of skew-symmetric matrices be possible, it is necessary that the ring be at least an F-ring.

Open Question: Let R be a commutative F-ring over which reduction of skew-symmetric matrices is possible. Is it necessary that R be a Hermite ring?

3.6 Elementary Divisor Rings

In this section, we are goingto consider the possibility of diagonal reduction.

Let us recall the following definitions. A matrix A admits a diagonal reduction if there exist non-singular matrices P and Q such that

$$PAQ = \text{diag}\,(d_1, d_2, \ldots)$$

and d_i is a divisor of d_{i+1}. A ring is called an elementary divisor ring if every matrix over it admits a diagonal reduction.

Let us note first that for row or column matrices diagonal reduction is equivalent to triangular reduction.

The following theorem shows the new difficulties are already embodied in the 2 by 2 case.

3.6.1 Theorem [K]: Let R be a commutative ring. If all 1 by 2, 2 by 1 and 2 by 2 matrices over R admit diagonal reduction. Then all matrices admit diagonal reduction and therefore R isan elementary divisor ring

Proof: Let $A = (a_{ij})$ be an m by n matrix. We may assume $m \geq n$ (by adding zero rows if necessary). We use induction, and suppose that the diagonal reduction is possible for all smaller m and the given m if $n < m$.

For $m \leq 2$ the hypothesis assures diagonal reduction, hence we assume $m \geq 3$. Write A_1 for the first row and A_2 for the rest. By induction we can find two non-singular matrix P_1 and Q_1 such that

$$B = P_1 A_2 Q_1$$

$$= \text{diag}\,(x_1, x_2, \ldots)$$

where $x_i | x_{i+1}$, then

$$C = \begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} Q_1$$

$$= \begin{pmatrix} A_1 \\ P_1 A_2 \end{pmatrix} Q_1$$

$$= \begin{pmatrix} A_1 Q_1 \\ P_1 A_2 Q_1 \end{pmatrix}$$

$$= \begin{pmatrix} A_1 Q_1 \\ B \end{pmatrix}$$

Let D be the first two rows of C and E be the remainder. Apply induction hypothesis to D, we have two non-singular matrices P_2 and Q_2 such that

$$F = P_2 D\, Q_2$$

$$= \begin{pmatrix} y & 0 & 0 & \dots & 0 \\ 0 & z & 0 & \dots & 0 \end{pmatrix}$$

where $y \mid z$, and hence

$$H = \begin{pmatrix} P_2 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} D \\ E \end{pmatrix} Q_2$$

$$= \begin{pmatrix} F \\ G \end{pmatrix},$$

where y divides all the entries of F.

Since $D = P_2^{-1} F Q_2^{-1}$ y also divides all the entries of D. The entries of G are linear combinations of E since

$$EQ_2 = G.$$

The entries of B are divisible by x. The entries of E which is the matrix B with the first row deleted, are divisble by x. Consequently the entries of G are divisble by x.

Now, y is a divisor of all entries of D and x is one of the element of D, hence y divides x also. Thus we conclude:

(i) y divides all entries of F

(ii) y divides all entries of G (since x divides all entries of G).

Thus y divides every entries of H.

Note

$$H = \begin{pmatrix} F \\ G \end{pmatrix} = \begin{pmatrix} y & 0 & & \dots & 0 \\ 0 & z & 0 & \dots & 0 \\ & & G & & \end{pmatrix}$$

Now, we may use elementary transformation to sweep out the first column of H and we reach $\begin{pmatrix} y & 0 \\ 0 & k \end{pmatrix}$ where K is m-1 by n-1 matrix and y still is a divisor of all the entries of K.

We apply induction to K. Therefore there exist two non-singular matrices P and Q such that

$$PKQ = \text{diag}\,(z_1,\dots,z_{n-1})$$

and $z_i | z_{i+1}$ then

$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & K \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & \text{diag}\,(z_1, z_2, \dots, z_{n-1}) \end{pmatrix}$$

Since y divides all z_i's, then the proof of the theorem is complete.

Before studying elementary divisor rings we need some more preparatory results.

3.6.2 Lemma [K]: Let R be a commutative ring and $a, b \in R$. Suppose u, v, s, t and $d \in R$ such that

$$a = ud \,, \quad b = vd \quad \text{and}$$

$$su + tv = 1$$

(hence $(a, b) = (d)$). Suppose $(a, b) = (d')$ where $d' \in R$. Then there exist u', v', s' and $t' \in R$ such that

$$a = u'd' \quad , \quad b = v'd' \quad \text{and}$$

$$s'u' + t'v' = 1 .$$

Proof: Since $(d) = (d')$. Let $d = kd'$ and $d' = \ell d$ where $k, \ell \in R$. Define $u' = k\ell t - t + uk$ and

$$v' = s - k\ell s + vk.$$

$$\begin{aligned} u'd' &= (k\ell t - t + uk)\, d' = k\ell td' - td' + ukd' \\ &= d\ell t - t\ell d + ud \\ &= ud \\ &= a \end{aligned}$$

$$\begin{aligned} v'd' &= (s - k\ell s + vk)\,(d') = sd' - k\ell sd' + vkd' \\ &= s\ell d - \ell sd + vd \\ &= vd \\ &= b \end{aligned}$$

Take $s' = s\ell - v$ and $t' = t\ell + u$

Therefore

$$\begin{aligned} s'u' + t'v' &= (s\ell - v)\,(u') + (t\ell + u)\,(v') \\ &= s\ell u' - vu' + t\ell v' + uv' \\ &= s\ell(k\ell t - t + uk) - v\,(k\ell t - t + uk) + \\ &\quad t\ell(s - k\ell s + vk) + u\,(s - k\ell s + vk) \end{aligned}$$

$$= s\ell k\ell t - s\ell t + s\ell uk - vk\ell t + vt - vuk +$$
$$t\ell s - t\ell k\ell s + t\ell vk + us - uk\ell s + uvk$$
$$= vt + us$$
$$= 1$$

3.6.3 Corollary: Let a, b, c be elements of a commutative ring R. Suppose R satisfies condition 'T' (Theorem 3.2.6). Then there exist d, u, v and w ϵ R such that

$$a = ud \quad , \quad b = vd \quad , \quad c = wd \quad \text{and}$$
$$(u, v, w) = 1.$$

Proof: Let us apply condition 'T' for a and b, i.e., there exist elements e, u', v', α and $\beta \epsilon R$ such that

$$\alpha u' + \beta v' = 1 \qquad \text{--- (1)}$$
$$u'e = a \quad \text{and} \quad b = ev'.$$

Note that condition 'T' implies that finitely generated ideals are principal. Therefore (a, b, c) = (d).

Now, (a, b) = (e). We also apply condition 'T' on e and c. Let $\bar{d}$ be the element such that (e, c) = ($\bar{d}$). Therefore ((a, b), c) = (e, c) = ($\bar{d}$) = (d).

By Lemma 3.6.2, we might as well take $\bar{d} = d$ and continue. Hence, let

$$(e, f) = (d) \quad \text{and}$$
$$e = fd \, , \quad c = wd \quad \text{and}$$
$$\gamma f + \delta w = 1 \qquad \text{--- (2)}$$

for some $f, w, \gamma, \delta \in R$.

Let $u = u'f$ and $v = v'f$, then

$$a = u'e = u'fd = ud$$

Similarly, $b = v'e = v'fd = vd$, and $c = wd$.

Now multiply (1) and (2)

$$(\alpha u' + \beta v')(\gamma f + \delta w) = \alpha u'\gamma f + \alpha u'\delta w + \beta v'\gamma f + \beta v'\delta w$$

$$= (\alpha\gamma)u + (\alpha u'\delta + \beta v'\delta)\, w + (\beta\gamma)\, v$$

$$= 1$$

Now we come to the important theorem due to $[G, H]_1$ which gives a characterization of an elementary divisor ring.

3.6.4 Theorem $[G, H]_1$: Let R be a commutative ring with identity, then it is an elementary divisor ring if and only if it satisfies the following two conditions

D_1. R is a Hermite ring

D_2. for any three elements $a, b, c \in R$ with $(a, b, c) = 1$ there exist $p, q \in R$ such that

$$(pa, pb + qc) = (1).$$

Proof: Suppose R is an elementary divisor ring, then every matrix admits diagonal reduction. So, in particular, every 1 by 2 and 2 by 1 matrix admits diagonal reduction, then R is a Hermite ring.

To prove the necessity of the second condition, let a,b,c be the given elements such that

$$(a, b, c) = 1.$$

Consider the matrix

$$A = \begin{pmatrix} a & b \\ o & c \end{pmatrix}$$

Suppose P and Q are the non-singular matrices such that

$$PAQ = \text{diag}\,(a_1, a_2) \quad \text{and} \quad a_1 | a_2 .$$

let $$P = \begin{pmatrix} p & q \\ r & s \end{pmatrix} , \quad Q = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

then

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & b \\ o & c \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

$$= \begin{pmatrix} pax + pbz + qcz & pay + pbt + qct \\ rax + rbz + scz & ray + rbt + sct \end{pmatrix}$$

Since R is Hermite let $(d) = (a_1, a_2)$. Therefore

$$d | a_1 \ , \quad d | a_2$$

i.e., d divides all entries of PAQ. Therefore d divides all entries of A. Hence d must be a unit since $(a, b, c) = 1$. Furthermore, since $a_1 | a_2$,

$$d = a_1 = (ap)\,(x) + (pb + qc)\,(z).$$

Now for the sufficiency, it is enough to show that any 2 by 2 matrix

admits diagonal reduction (Theorem 3.6.1).

Let $A = \begin{pmatrix} a & b \\ d & c \end{pmatrix}$ be a 2 by 2 matrix. Since the ring is Hermite A admits a triangular reduction. Hence we may assume $d = 0$.

Now, let $(a, b, c) = (e)$, e cannot be zero because otherwise the matrix $A = 0$. By corollary 3.6.3 there exist $u, v, w, x, y, z \in R$ such that

$$a = ue, \quad b = ve, \quad c = we \quad \text{and}$$

$$xu + yv + zw = 1.$$

So

$$A = \begin{pmatrix} e & o \\ o & e \end{pmatrix} \begin{pmatrix} u & v \\ o & w \end{pmatrix} \quad \text{and}$$

$\begin{pmatrix} e & o \\ o & e \end{pmatrix}$ is a scalar matrix it commutes with any matrix.

Hence it is enough to find diagonal reduction for $\begin{pmatrix} u & v \\ o & w \end{pmatrix}$.

Consequently without loss of generality we may assume our matrix A is of the form:

$$A = \begin{pmatrix} a & b \\ o & c \end{pmatrix}$$

with $(a, b, c) = 1$. Therefore by D_2 there exist $p, q \in R$ such that $(pa, pb + qc) = (1)$.

Note $(p, q) = (1)$, hence there exist $x, y \in R$ such that

$$px + qy = 1,$$

also there exist $u, v \in R$ such that

$$u(pa) + v(pb + qc) = 1.$$

Let $P = \begin{pmatrix} p & q \\ -y & +x \end{pmatrix}$ and $Q = \begin{pmatrix} u & -(pb+qc) \\ +v & +pa \end{pmatrix}$

then P and Q are non-singular and

$$PAQ = \begin{pmatrix} p & q \\ -y & x \end{pmatrix} \begin{pmatrix} a & b \\ o & c \end{pmatrix} \begin{pmatrix} u & -(pb+qc) \\ v & pa \end{pmatrix}$$

$$= \begin{pmatrix} pa & pb+qc \\ -ya & -yb+xc \end{pmatrix} \begin{pmatrix} u & -(pb+qc) \\ v & pa \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ \cdots\cdots & \end{pmatrix}$$

Now this matrix can be diagonalized by sweeping out the first element in the second row.

Remark: There exist examples of Hermite rings which are not elementary divisor rings and examples of F-ring, which are not Hermite.

We describe the following example due to Gillman and Henriksen (for details see $[G, H]_2$ example 4.11 page 382).

3.6.5 Example: Let X be the topological space $= R^+ \cup S^+$ where

$R^+ = \{(x, 0) \mid x \geq 0\}$ and

$S^+ = \{(x, \sin\pi x) \mid x \geq 0\}$,

then the ring of continuous functions over $\beta X - X$, where β is the Stone-čech compactification, is a Hermite ring but not an elementary

divisor ring.

3.6.6 Example: Let X denote the strip of the Eucledian plane $\{(x, y) \mid x \geq 0, |y| \leq 1\}$. Let Y be the topological space $\beta X - X$ then the ring of continuous functions over Y is an F-ring but not a Hermite ring. For more details see $[G, H]_2$ example 3.4 page 378.

Remark: The above two examples are of topological nature, so it will be interesting and instructive to find examples of F-rings which are not Hermite rings and examples of Hermite ring which are not elementary divisor rings without using topology.

3.7 Conclusion

In this concluding section we show that the class of elementary divisor rings is fairly large by showing that a Von Newmann regular ring is an elementary divisor ring.

3.7.1 Definition: A commutative ring R with identity is said to be a Von Neumann regular ring if for every $a \in R$ there exist an $x \in R$ such that $a^2x = a$.

3.7.2 Example: Let I be an index set and k_i be a field for each i. Let $R = \prod_{i \in I} k_i$, hence

$$R = \{f \mid f : I \to \bigcup_{i \in I} k_i, \quad f(i) \in k_i\}$$

let $f \in R$, we define x as follows

$$x(i) = \begin{cases} f^{-1}(i) & \text{if } f(i) \neq 0 \\ 0 & \text{if } f(i) = 0 \end{cases}$$

clearly x is an element of R.

We claim $f^2x = f$.

If $f(i) \neq 0 \Rightarrow f^2x = f^2(i)\, f^{-1}(i) = f(i)$

If $f(i) = 0 \Rightarrow f^2x = f = 0$

The above example shows that the class of Von Neumann regular ring is very large.

First we give below some properties of Von-Neumann regular rings.

3.7.3 Proposition: Let R be a Von Neumann regular ring. Then every principal ideal is generated by an idempotent element.

Proof: Let $a \in R$. Consider the principal ideal generated by a. By hypotheses there exist x such that $xa^2 = a$. Consider $xa = e$. Then

$$e^2 = (xa)\,(xa) = (x)\,(xa^2) = xa = e$$

Therefore e is an idempotent.

Now, $(a) = (e)$, for $e = ax$ and

$$a = a^2x = a(ax) = ae\,.$$

3.7.4 Theorem: Every Von Neumann ring is an F-ring.

Proof: Let $a, b \in R$, let $x, y \in R$ such that

$$a^2x = a, \quad b^2y = b.$$

Let $e = ax$, $f = by$ and $d = e + f - ef$. Then

$$a = ad, \quad b = bd \text{ and } d \in (e, f) = (a, b) \qquad \text{--- (1)}$$

For $$ad = ae + af - aef = a + af - af = a, \qquad \text{--- (2)}$$

Similarly

$$bd = be + bf - bef = be + bf - be = bf = b \qquad \text{--- (3)}$$

($ae = a$ and $bf = b$). By 3.7.3

$$(a) = (e), \quad (b) = (f) \text{ and } (a, b) = (e, f).$$

Equations (1), (2) and (3) show that $(a, b) = (e,f) = (d)$.

3.7.5 Proposition: For any element a of a Von-Neumann regular ring R there exists a unit u such that

$$a^2u = a.$$

Proof: Let x satisfy $a^2x = a$. Let $z \in R$ such that $x^2z = x$. Define $u = 1 + x - xz$. Note

$$axz = (a^2x)(xz) = a^2(x^2z) = a^2x = a$$

$$a^2u = a^2(1 + x - xz) = a^2 + a^2x - a^2xz$$

$$= a^2 + a - a(axz) = a^2 + a - a^2 = a$$

Since $u + (z - 1)x = 1$, then $(u, x) = 1$. But $xu = x^2$, for

$$\begin{aligned} xu &= x(1 + x - xz) \\ &= x + x^2 - x^2z \\ &= x + x^2 - x \\ &= x^2 \end{aligned}$$

If M is a maximal ideal which contains u, then M contains $xu = x^2$. Since M is also a prime ideal it must contain x. Hence every maximal ideal which contains u must contain x, therefore that maximal ideal contains 1. Therefore no maximal ideal contains u hence u is a unit.

3.7.6 Definition: Let R be a commutative ring with identity, R is called adequate if it is

(1) an F-ring and

(2) The following condition is satisfied

'A' for every $a, b \in R$ $a \neq 0$, there exist $u, d \in R$ such that

(i) $a = ud$ and (ii) $(u, b) = (1)$ and

for every non-unit divisor e of d $(e, b) \neq (1)$.

Remark: The ring of entire functions is an adequate ring. For more details see Helmer $[H]_2$.

The following theorem is due to Gillmann and Henriksen.

3.7.7 Theorem: An adequate ring is an elementary divisor ring iff it is an Hermite ring.

Proof: Since every elementary divisor ring is a Hermite ring we have only to show that an adequate Hermite ring is an elementary divisor ring. We have to verify condition D_2 in Theorem 3.6.4. Suppose $a, b, c \in R$ such that $(a, b, c) = 1$, we want to find p and q such that

$$(pa, pb + qc) = (1).$$

If $a = 0$, there is nothing to prove. Assume $a \neq 0$. Write $a = rs$ by applying property 'A' for the elements a and c in Definition 3.7.6 with $(r, c) = (1)$ so let $sr + tc = 1$ and take $q = t(1 - b)$.

Consider
$$\begin{aligned} b + qc &= b + t(1 - b)c \\ &= b + tc - tbc \\ &= b + (1 - sr) - tbc \\ &= b + 1 - sr - btc \\ &= b(1 - tc) - sr + 1 \\ &= bsr - sr + 1 = sr(b - 1) + 1 \end{aligned}$$

Let $d = (a, b + qc)$. Now if $x|d$ and $x|r$ hence $x|a$ then $x|b + qc$ and $x|r$ therefore $x|1$ (by above equation). Thus $(d, r) = 1$ and it follows from $a = rs$ and $(d, r) = 1$ then $d|a \Rightarrow d|s$. So if d is not a unit then $(d, c) \neq 1$ (by applying property 'A' to a and c). If $(d, c) \neq 1$, let $y \neq 1$ be a divisor of d and c

then $y|a$, $y|c$ hence $y|b$ from

$$d = (a, b + qc)$$

But $(a, b, c) = 1$ hence $y = 1$. Therefore the only divisor of d and $c = 1$. So $(d, c) = 1$. Hence we have contradiction.

3.7.8 Theorem [G, H]$_1$: Every Von Neumann regular ring is adequate.

Proof: Let R be a Von Neumann regular ring then by Theorem 3.7.4 it is an F-ring. Therefore we have to verify condition 'A' in Definition 3.7.6.

Let $a, b \in R$, $a \neq 0$, then by Proposition 3.7.5 there exist $u, v \in R$ where u and v are units such that $a^2u = a$ and $b^2v = b$.

Now, $e = au$ and $f = bv$ are idempotents (by proposition 3.7.3). We may work instead with the idempotent e and f of which a and b are unit multiples. Note also that

$$(a, b) = (d)$$
$$= (e, f)$$

where $d = e + f - ef$ and put

$$e_1 = 1 - f + ef \qquad \text{--- 1}$$

Then $e = e_1d$, for

$$(e + f - ef)(1 - f + ef) = e+f-ef-ef-f^2+ef^2+e^2f+ef^2-e^2f^2$$
$$= e+f-ef-ef-f+ef+ef+ef-ef$$
$$= e.$$

From (1)

$$e_1 + (1 - e) f = 1.$$

Therefore

$$(e_1, f) = 1.$$

Now, $d|f$ so no non-unitdivisor d' of d can be relatively prime to f (i.e., $(d', f) \neq (1)$ for any non-unit divisor of d.

3.7.9 Theorem: Every Von Neumann regular ring is a Hermite ring.

Proof: Let $a, b \in R$, we must verify 'T' condition (Theorem 3.2.6). As in the discussion of the previous theorem it is enough to verify the 'T' condition for the corresponding idempotents e and f. Let $d = e + f - ef$, take $u = 1 - f + ef$ and $v = f$. Then $e = ud$ and $f = vd$. Note that we proved in 3.7.8 $(e, f) = 1$. Therefore $(u, v) = 1$, hence there exist $s, t \in R$ such that

$$su + tv = 1.$$

3.7.10 Corollary: Every Von Neumann regular ring is an elementary divisor ring.

Proof: Follows from 3.7.7, 3.7.8 and 3.7.9.

REFERENCES

[A-M] Atiyah-Macdonald: Introduction to commutative Algebra; Addison-Wesly, (1969).

[B] Jacob Barshay: Topics in Ring Theory; W.A. Benjamin Inc. (1969).

[C] P.M. Cohn: Algebra Volume 1; John Wiley & Sons (1974).

$[G\text{-}H]_1$ L. Gillman and M. Hendriksen; Some remarks about elementary divisor ring; Trans. Amer. Math. Soc. 82 (1956), 362-365.

[G] R. Godement: Algebra; Kershaw Publishing Company Ltd., London (1969).

[Hu] T.W. Hangerford: Algebra; Holt, Rinehart and Winston, Inc. (1974).

[K] I. Kaplansky: EElementary divisors and modules; Trans. Amer. Math. Soc. 66 (1949), 464-491.

$[G\text{-}H]_2$ L. Gillman and M. Hendriksen: Rings of Continuous functions in which every finitely generated ideal is principal; Trans. Amer. Math. Soc. 82 (1956), 366-391.

[M] Kurt Meyberg: Algebra; Teil 1, Carl Hanser Verlag Munchen Wien 1975, Section 3.6 from page 133 to 141 translated by Dr. Fakhruddin.

$[H]_1$ OLF Helmer: The Elementary Divisor Theorem for Certain Rings without Chain Condition; Bull. Amer. Math. Soc. Vol. 49 (1943) 225-236

$[H]_2$ O. Helmer: "Divisibility properties of integral functions," Duke Math. J. 6 (1940), 345-356.

[N] D.G. Northcott: Ideal Theory; Cambridge University Press (1965).

الحمد لله رب العالمين